We encourage you to e-mail your comments to us at: strategicstudiesquarterly@maxwell.af.mil.

SSQ

STRATEGIC STUDIES QUARTERLY

SPRING 2011 VOL. 5, NO. 1

AIR UNIVERSITY

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2011		**00-00-2011 to 00-00-2011**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Strategic Studies Quarterly. Volume 5, Number 1, Spring 2011	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air University,Strategic Studies Quarterly,155 N. Twining St,Maxwell AFB,AL,36112-6025**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**156**	

Strategic Studies Quarterly (*SSQ*) (ISSN 1936-1815) is published quarterly by Air University Press, Maxwell AFB, AL.

Strategic Studies Quarterly

An Air Force–Sponsored Strategic Forum on National and International Security

VOLUME 5 SPRING 2011 NUMBER 1

Commentary

Part I

Feature Article

Perspectives

Book Reviews

Part II

On-line Version

Blown to Bits: China's War in Cyberspace, August-September 2020
Christopher Bronk
http://www.au.af.mil/au/ssq/2011/spring/bronk.pdf

Cyberdeterrence between Nation-States: Plausible Strategy or a Pipe Dream?
Jonathan Solomon
http://www.au.af.mil/au/ssq/2011/spring/solomon.pdf

Cyber Glossaries

Glossary of Security Terms
The SANS Institute
http://www.sans.org/security-resources/glossary-of-terms

National Information Assurance (IA) Glossary
Committee on National Security Systems (CNSS)
http://www.ecs.csus.edu/csc/iac/cnssi_4009.pdf

The Future of Things "Cyber"

Years ago, when I was an ROTC instructor, the first unit of instruction for rising juniors dealt with communication skills. Near the beginning of the unit, I would quote Confucius to my new students: "The rectification of names is the most important business of government. If names are not correct, language will not be in accordance with the truth of things." The point had less to do with communicating than it did with thinking—thinking clearly. Clear communication begins with clear thinking. You have to be precise in your language and have the big ideas right if you are going to accomplish anything.

I am reminded of that lesson as I witness and participate in discussions about the future of things "cyber." Rarely has something been so important and so talked about with less clarity and less apparent understanding than this phenomenon. Do not get me wrong. There are genuine experts, and most of us know about patches, insider threats, worms, Trojans, WikiLeaks, and Stuxnet. But few of us (myself included) have created the broad structural framework within which to comfortably and confidently place these varied phenomena. And that matters. I have sat in *very* small group meetings in Washington, been briefed on an operational need and an operational solution, and been unable (along with my colleagues) to decide on a course of action because we lacked a clear picture of the long-term legal and policy implications of *any* decision we might make.

US Cyber Command has been in existence for more than a year, and no one familiar with the command or its mission believes our current policy, law, or doctrine is adequate to our needs or our capabilities. Most disappointingly—the doctrinal, policy, and legal dilemmas we currently face remain unresolved even though they have been around for the better part of a decade. Now is the time to think about and force some issues that have been delayed too long. This edition of *Strategic Studies Quarterly*, therefore, could not be more timely as it surfaces questions, fosters debate, and builds understanding around a host of cyber questions. The issues are nearly limitless, and many others will emerge in these pages, but let me suggest a few that frequently come to the top of my own list.

How do we deal with the unprecedented? Part of our cyber policy problem is that its newness and our familiar experience in physical space do not easily transfer to cyberspace. Casually applying well-known concepts

from physical space like deterrence, where attribution is assumed, to cyberspace where attribution is frequently *the* problem, is a recipe for failure. And cyber education is difficult. In those small–group policy meetings, the solitary cyber expert often sounds like "Rain Man" to the policy wonks in the room after the third or fourth sentence. As a result, no two policymakers seemed to leave the room with the same understanding of what it was they had discussed, approved, or disapproved. So how do we create senior leaders—military and civilian who are "cyber smart enough"?

Is cyber really a domain? Like everyone else who is or has been in a US military uniform, I think of cyber as a domain. It is now enshrined in doctrine: land, sea, air, space, *cyber*. It trips off the tongue, and frankly I have found the concept liberating when I think about operationalizing this domain. But the other domains are natural, created by God, and this one is the creation of man. Man can actually change this geography, and *anything* that happens there actually creates a change in someone's *physical* space. Are these differences important enough for us to rethink our doctrine? There are those in the US government who think treating cyber as an independent domain is just a device to cleverly mask serious unanswered questions of sovereignty when conducting cyber operations. They want to be heard and satisfied before they support the full range of our cyber potential.

Privacy? When we plan for operations in a domain where adversary and friendly data coexist, we should be asking: What constitutes a twenty-first-century definition of a reasonable expectation of privacy? Google and Facebook know a lot more about most of us than we are comfortable sharing with the government. In a private-sector web culture that seems to elevate transparency to unprecedented levels, what is the appropriate role of government and the DoD? If we agree to limit government access to the web out of concerns over privacy, what degree of risk to our own security and that of the network are we prepared to accept? How do we articulate that risk to a skeptical public, and who should do it?

Do we really know the threat? Former Director of National Intelligence Mike McConnell frequently says we are already "at war" in cyberspace. Richard Clarke even titled his most recent cautionary book, *Cyber War*. Although I generally avoid the *at war* terminology, I often talk about the inherent insecurity of the web. How bad is it? And if it is really bad, with the cost of admission so low and networks so vulnerable, why have we not had a true cyber Pearl Harbor? Is this harder to do than we think? Or, are we just awaiting the inevitable? When speaking of the threat, citizens of a

series of first-world nations were recently asked whom they feared most in cyberspace, and the most popular answer was not China or India or France or Israel. It was the United States. Why is that, and is it a good thing? People with money on the line in both the commercial and government sectors want clear, demonstrable answers.

What should we expect from the private sector? We all realize that most of the web things we hold dear personally and as a nation reside or travel on commercial rather than government networks. So what motivates the private sector to optimize the defense of these networks? Some have observed that the free market has failed to provide an adequate level of security for the net since the true costs of insecurity are hidden or not understood. I agree. Now what: liability statutes that create the incentives and disincentives the market seems to be lacking? Government intervention, including a broader DoD role to protect critical infrastructure beyond .mil to .gov to .com? The statutory responsibility for the latter falls to the Department of Homeland Security, but does it have the "horses" to accomplish this? Do we await catastrophe before calling for DoD intervention, or do we move preemptively?

What is classified? Let me be clear: This stuff is overprotected. It is far easier to learn about physical threats from US government agencies than to learn about cyber threats. In the popular culture, the availability of 10,000 applications for my smart phone is viewed as an unalloyed good. It is not—since each represents a potential vulnerability. But if we want to shift the popular culture, we need a broader flow of information to corporations and individuals to educate them on the threat. To do that we need to recalibrate what is truly secret. Our most pressing need is clear policy, formed by shared consensus, shaped by informed discussion, and created by a *common* body of knowledge. With no common knowledge, no meaningful discussion, and no consensus . . . the policy vacuum continues. This will not be easy, and in the wake of WikiLeaks it will require courage; but, it is essential and should itself be the subject of intense discussion. Who will step up to lead?

What constitutes the right of self defense? How much do we want to allow private entities to defend themselves outside of their own perimeters? Indeed, what should Google appropriately do *within* its own network when under attack from the Chinese state? I have compared our entry into cyberspace to mankind's last great era of discovery—European colonization of the Western Hemisphere. During that period, large private corporations like the Hudson Bay Company and the East India Tea Company acted

with many of the attributes of sovereignty. What of that experience is instructive today for contemplating the appropriate roles of giants like Google and Facebook? We probably do not want to outfit twenty-first-century cyber privateers with letters of marque and reprisal, but what should be the relationship between large corporations and the government when private networks on which the government depends are under sustained attack?

Is there a role for international law? It took a decade last century for states to arrive at a new Law of the Seas Convention, and that was a domain our species had had literally millennia of experience. Then, as a powerful seafaring nation, we tilted toward maritime freedom rather than restraints. Regulating cyberspace entails even greater challenges. Indeed, as a powerful cyberfaring nation, how comfortable are we with regulation at all? After all, this domain launched by the DoD has largely been nurtured free of government regulation. Its strengths are its spontaneity, its creativity, its boundlessness. The best speech given by an American official on macro net policy was given late last year by Secretary of State Clinton when she emphasized Internet freedom, not security or control or regulation. But there are moves afoot in international bodies like the International Telecommunications Union to regulate the Internet, to give states more control over their domains, to Balkanize what up until now has been a relatively seamless global enterprise. How and when do we play?

Is cyber arms control possible? As a nation, we tend toward more freedom and less control but—given their destructiveness, their relative ease of use, and the precedent their use sets—are distributed denial-of-service attacks *ever* justified? Should we work to create a global attitude toward them comparable to the existing view toward chemical or biological weapons? Should we hold states responsible if an attack is mounted from their physical space even if there is no evidence of complicity? And, are there *any* legitimate uses for *botnets*? If not, under what authority would anyone preemptively take them down? These are questions for which no precedent in law or policy (domestic or international) currently exists. If we want to establish precedent, as opposed to likely unenforceable treaty obligations, do we emphasize dialogue with like-minded nations, international institutions . . . or multinational IT companies?

Is defense possible? At a recent conference, I was struck by a surprising question: "Would it be more effective to deal with recovery than with prevention?" In other words, is the web so skewed toward advantage for

the attacker that we are reaching the point of diminishing returns for defending a network at the perimeter (or even beyond) and should now concentrate on how we respond to and recover from inevitable penetrations? This could mean more looking at *our* network for anomalous behavior than attempting to detect every incoming zero–day assault. It could mean concentrating more on what is going out rather than what is coming in. It could mean more focus on mitigating effects and operating while under attack rather than preventing attack. Mike McConnell and I met with a group of investors late last year, and we were full-throated in our warnings about the cyber threat. One participant asked the question that was clearly on everyone's mind, "How much is this going to cost me?" At the time I chalked it up to not really understanding the threat, but in retrospect our questioner may have been on to something. At what point do we shift from additional investment in defense to more investment in response and recovery?

There are more questions that could be asked, many of them as fundamental as these. Most we have not yet answered or at least have not yet *agreed* on answers, and none of them are easy. How much do we really want to empower private enterprises to defend themselves? Do we want necessarily secretive organizations like NSA or CyberCom going to the mats publicly over privacy issues? At what point does arguing for Internet security begin to legitimate China's attempts at control over Internet speech? Do we really want to get into a public debate that attempts to distinguish cyber espionage (which all countries pursue) from cyber war (something more rare and *sometimes* more destructive)? Are there any cyber capabilities, real or potential, that we are willing to give up in return for similar commitments from others?

Tough questions all—tougher (perhaps) but not unlike those our airpower ancestors faced nearly a century ago. As pioneer air warriors grappled with the unfamiliar, so must we. Until these and other questions like them are answered, we could be forced to live in the worst of all possible cyber worlds—routinely vulnerable to attack and self-restrained from bringing our own power to bear.

Gen Michael V. Hayden, USAF, Retired
Former Director, National Security Agency
Former Director, Central Intelligence Agency

An Air Force Strategic Vision for 2020–2030

John A. Shaud, General, USAF, Retired
Adam B. Lowther

Two decades of continuous operations that began with Desert Shield/Desert Storm (1990–91) and continued to the conflicts in Afghanistan and Iraq have resulted in Airmen engaged in responding to current operations, leaving little time to contemplate the longer-term strategic imperatives that will influence the future force structure of the United States Air Force. With Operation Iraqi Freedom recently coming to an end and troop reductions in Afghanistan scheduled to begin this year, it is both timely and appropriate to reinvigorate strategic thought within the Air Force. This article seeks to stimulate a discussion concerning the Air Force's future by addressing a single question: What critical capabilities—through combatant commanders' lenses—will the nation require of the Air Force by 2030?

To answer this question, the Air Force Research Institute analyzed national interests; economic, demographic, and technological trends; defense scenarios spanning the strategic planning space; and Air Force capabilities required to meet future strategic challenges.[1] Research was conducted using futures analysis methods and the Delphi method. The resulting analysis of these issues appears in *Air Force Strategy Study 2020–2030.* Its findings suggest the Air Force should focus on five critical capabilities over the next two decades: (1) power projection, (2) freedom of action in air, space, and cyberspace, (3) global situational awareness,

---

Gen John A. Shaud, PhD, USAF, retired, is director, Air Force Research Institute, Maxwell AFB, Alabama, where he directs an 80-person organization charged with conducting independent research, outreach, and engagement to enhance national security and assure the effectiveness of the US Air Force. He provides guidance to a team of 15 operationally savvy researchers; the Air University Press, and Air University research and conference support. General Shaud also supervises production of the *Strategic Studies Quarterly* and the *Air and Space Power Journals*, the latter published quarterly in six languages and distributed worldwide.

Adam Lowther, PhD, is a faculty researcher and defense analyst at the Air Force Research Institute, Maxwell AFB. He is the author of *Americans and Asymmetric Conflict: Lebanon, Somalia, and Afghanistan* (Praeger, 2007) and co-editor of *Terrorism's Unanswered Questions* (Greenwood, 2009). Dr. Lowther served in the US Navy from 1994 to 2001 aboard the USS *Ramage* (DDG-61) and at CINCUSNAVEUR, London.

(4) air diplomacy, and (5) military support to civil authorities (MSCA). There is also an underlying theme that runs throughout the study. Success—for the Air Force—will depend on the service's ability to integrate the application of American power through the air, space, and cyber domains. No longer is it possible to think or act principally in a single domain. Actors—friend or foe—who are most effective in operating across domains will achieve their objectives with greater frequency than those who remain stuck in a paradigm that is focused on a single domain.

Air Force Critical Capabilities 2020–2030

The geostrategic environment the United States will face in 2030 is certain to pose challenges that diverge significantly from those the nation and the Air Force face today. To begin with, the United States' focus is likely to continue shifting from Europe to Asia, which will require a greater emphasis on long-range power projection by the Air Force.[2] Defense of national interests in Asia—thought of by many as the twenty-first century's center of commerce and power—will double, in most cases, the distances the Air Force must fly to reach its primary operating areas. This challenge will require innovative thinking if the United States and the Air Force are to maintain regional influence during a time of expected stagnant or declining defense budgets. Continued success will likely come through the integration of cyber and space—particularly important in an Asia-centered world. With this brief description of the strategic landscape in mind, the following pages discuss each of the five capabilities determined to be most critical for the Air Force to develop or enhance between the present and 2030.

Power Projection

The United States faces humanitarian disasters, resource conflicts, terrorism, small-scale conventional conflicts, insurgencies, and the potential for peer conflicts. Flexible power projection is certain to prove critical to American success in these conflicts. In a global security environment marked by the proliferation of advanced antiaccess and area denial (A2/AD) systems, American forces will find it increasingly difficult to establish secure bases within striking distance of adversaries.[3] This will increase the demand for long-range power projection options. Successful power

projection is undoubtedly the most critical capability the Air Force will provide combatant commanders and the nation.[4]

For the Air Force, power projection can take many forms—as either hard or soft power. While power projection is synonymous with capabilities such as penetrating long-range strike, airlift, and aerial refueling, the future will also call for something new to the Air Force—offensive cyber capabilities. As the Air Force moves forward, the force structure—and, consequently, force-development programs—must change to emphasize these requirements, which will include integrating (manned and unmanned) air, space, and cyber capabilities. In other words, when formulating options to defend the nation's interests, Airmen should present choices that represent the full range of integrated capabilities.

This approach will position the service to capitalize on technological developments before and after 2030. Near-term changes in organization, doctrine, training, education, and force management will be required. For example, the current requirements of rated personnel (six-, nine-, and 12-year flying gates) make it difficult to provide opportunities for them to acquire skills in space or cyber fields during their formative operational years. Providing limited exposure to traditional Air Force operations for individuals in the space and cyber career fields similarly undermines their understanding of airpower. By 2030, Airmen operating in a joint environment will be expected to present comprehensive options that represent the full capabilities of the Air Force rather than presenting compartmentalized solutions.

The key strategic problem from the perspective of potential adversaries is to deny the United States access to bases and targets. The proliferation of robust and redundant air defenses is a legacy of the Cold War, but this has taken on new importance for adversaries. In the near term, most nations will be unable to compete with the United States' technological advantages in conventional combat. However, this will change as 2030 approaches. Future battlefields may look more like the recent Russo-Georgian conflict, in which a cyber offensive preceded Russia's conventional attack. Conflicts will be more specifically targeted in terms of time and space, and the first salvos of a conflict may not be detected until the second- and third-order effects of initial strikes manifest themselves.

Rather than relying solely on traditional integrated air defenses, adversaries will compete for control of the air by 2030 using integrated denial strategies informed by space- and cyber-based surveillance, reconnaissance,

and attack coupled with high-performance, stealthy radar and missile systems designed to complicate deployment and operations for American airpower. As noted in the recent *Quadrennial Defense Review Report*, "The future operational landscape could also portend significant long-duration air and maritime campaigns for which the US Armed Forces must be prepared."[5] In these increasingly dangerous scenarios, Air Force capabilities will experience increased stress. The Air Force must present strategic and operational choices along with forces capable of operating and prevailing in environments where adversaries have unprecedented capability to deny American forces access.[6] As one analysis noted, "The USAF's path remains that of betting that forward bases, which are falling increasingly within the reach of enemy ballistic missiles, cruise missiles, and other A2 [antiaccess] capabilities, can nonetheless be utilized by its expeditionary air units."[7]

Conventional power projection against peer or near-peer competitors will continue to shape Air Force requirements for the foreseeable future.[8] Four recommendations are offered to assist the Air Force in meeting power-projection requirements across the strategic planning space during the next two decades.

First, the Air Force must begin the process of fusing air, space, and cyber capabilities into existing and future platforms and systems. For example, aircraft currently rely on the global positioning system (GPS)—a space asset—and a range of cyber systems, but much more is possible at the individual platform level and in support of command and control. Integrating capabilities, both offensive and defensive, across the three domains will prove a key enabler and force multiplier over the coming decades. This suggests the need for systems, operators, and organizations that are capable of achieving effects in more than one domain.

Second, the service must continue to refine a flexible power-projection capability. For example, in a conflict with a peer competitor, where national sovereignty and vital interests are threatened, the calculus for determining an appropriate Air Force response is simple. However, in an irregular conflict where limited interests are at stake, determining the appropriate course of action is more difficult. With Air Force power-projection capabilities often serving as the single best tool available, options must be scalable. This presents a challenge that is proving difficult to overcome in present conflicts.

In an irregular conflict, two potentially divergent Air Force missions are possible: fighting as a member of the joint or coalition force or enabling partners to fight on their own.[9] The former requires traditional airpower

assets. In the latter, the Air Force can leverage tools such as training, education, and assistance. The Air Force needs to develop "general purpose" forces accustomed to operating with allies in ways not often considered part of the service's power projection role.[10] Preserving combat capabilities for major contingencies will require greater investments in irregular warfare capabilities today. As Afghanistan and Iraq have demonstrated, the Air Force's most capable aircraft are not always necessary in an irregular conflict. By developing the appropriate capabilities for this mission, the service can achieve significant cost savings and preserve the utility of the nation's most capable aircraft.

Third, developing unmanned platforms that are enhanced by artificial intelligence—enabling autonomous operations—will support the Air Force conventional power projection mission. Such systems may prove critical psychological tools in peer competition, where an adversary may view the employment of such systems as a reason to cooperate with the United States. Extending the range and loiter time of existing and future platforms will have a similar effect.

Improving the range of air-breathing platforms will also delay or prevent the compromise of one of airpower's greatest advantages: the ability to operate from secure locations outside an adversary's reach. As American forces withdraw from Iraq and eventually Afghanistan, there will be a greater focus on Asia. Thus, the likely continuing drawdown in overseas forces and the number of OCONUS main operating bases must be offset not only through a closer relationship between the Air Force and Navy, but with long-range power-projection systems capable of holding targets at risk without access to nearby bases.

Fourth, offensive and defensive cyber capabilities must be fused into air and space platforms. By 2030 cyber capabilities may become the greatest power-projection tools in the Air Force arsenal, serving as both force multipliers and an Achilles' heel. Several nations are clearly equal to or ahead of the United States in their ability to launch cyber attacks. Despite the Air Force's attempts to organize, train, and equip to meet cyber requirements, its ability to conduct robust cyber operations remains a potential but not assured capability. As the discussion turns to the freedom of action in air, space, and cyberspace, these same challenges are present.

Freedom of Action in Air, Space, and Cyberspace

Although the previous section called for the integration of air, space, and cyber for the sake of improving power-projection capabilities, freedom of action in air, space, and cyberspace is not limited to playing a role in power projection. In other words, the five capabilities are neither mutually exclusive nor always complementary. This point is worth noting as the discussion turns to the continuing importance of air superiority.

Air

Access to and stability within the global commons (space, air, sea, and cyber domains) is critical to national security.[11] The objective of air superiority focuses on a subset of the larger challenge of access to all the global commons and ensuring access to the air domain at places and times of America's choosing. Air superiority also encompasses the ability to use the air domain to observe potential adversaries through reconnaissance and surveillance and then hold important targets at risk to influence outcomes in a way that is favorable to the United States.

Over the coming decades significant advances in air superiority are possible in the areas of autonomous systems and augmentation of human performance.[12] This may include stealthy, high-performance, autonomous aircraft that augment the numbers and capabilities of fifth-generation fighters and replace the lost contribution of legacy fighters relegated to supporting roles, "building the foundation provided by F-22s and F-35s" before they are phased out.[13]

Augmenting human performance can "achieve capability increases and cost savings via increased manpower efficiencies and reduced manpower needs."[14] This will prove useful as weapon systems become increasingly complex and dependent on advanced man-machine interfaces. It is reasonable to expect remotely piloted aircraft (RPA) to evolve into truly autonomous aircraft, increasing the number of air superiority missions and supporting tasks such platforms perform.

Improvements in the man-machine interface will continue to progress in speed, range, aerodynamic performance, sensor capabilities, information processing, and decision making. Current examples include infrared sensors to see at night, radar to see through weather, and computer interpretation of GPS signals for navigation. By 2030, the amount of information to be analyzed, the number of decisions to be made, and the rate at which they must be made will increase dramatically and further exceed

human capabilities, requiring significantly more capable man-machine systems.[15]

With the F-22 and F-35 likely to serve as the nation's principal air superiority platforms until 2030 and a reduction in the purchase of F-35s likely, relatively inexpensive force multipliers such as autonomous unmanned platforms, human-computer enhancements, and cyber-attack capabilities may become more important.[16] Along with the competing need for capital investment in long-range strike, there is a real need to recapitalize the nation's conventional and nuclear strategic defense systems. Thus, inexpensive force multipliers should be a focus of air superiority development. One such option is an aircraft-mounted cyber-attack system with the ability to penetrate and disrupt the software of an adversary's aircraft, radar, and other systems. However, cyber is an area where the United States has the slimmest advantage over some adversaries. Cyber is not a magic bullet, but an area where investments may pay significant dividends.

Adversaries of the United States are continuously developing new means of challenging American air superiority. Denying their success will require that the Air Force continually adapt to improving systems and changing tactics, techniques, and procedures. This will become increasingly difficult as competition for research and development dollars grows over the next two decades. As with air, space presents a distinct set of challenges.

Space

As a pioneer and leader in the use of space, the United States is more reliant on the domain than any other nation. Recognizing the significance of space, on 28 June 2010 the Obama administration issued a new space policy declaring that "the United States will employ a variety of measures to help assure the use of space for all responsible parties, and, consistent with the inherent right of self-defense, deter others from interference and attack, defend our space systems and contribute to the defense of allied space systems, and, if deterrence fails, defeat efforts to attack them."[17] To achieve this national priority, the Air Force must gain space superiority, a concept not unlike air or cyber superiority. Currently, however, the United States cannot maintain space superiority. Thus, the principal objective over the next 20 years must be to exert control over space in a way that turns the concept of space superiority into a reality.

While space is unlikely to become a domain through which kinetic effects are delivered in the near term, challenges to American preeminence

may accelerate deployment of weapons in space—dramatically altering the existing paradigm. Denying space to the United States would significantly degrade its civil and military operations in all domains. Events such as an attack on a communication, navigation, or detection constellation could drive a demand for weaponization by the American public, which would require the Department of Defense (DoD) to respond aggressively.

A successful strategy to delay the weaponization of space and maintain freedom of action in the domain will require that the United States use the entire spectrum of diplomatic, information, military, and economic capabilities to develop a multilayered construct for space operations. By masking the United States' space center of gravity, an adversary is placed in a defensive position. However, space superiority does not begin with a military solution. It starts with the United States taking the lead in engaging the international community to create a system of protocols and relationships that encourages beneficial and benign behavior. Through economic and technical cooperation such as trade and multinational research and development, nations become interdependent and much less likely to act against their own interests.[18]

Partnering also lays the foundation for international negotiation, regulation, and governance by the rule of law—powerful concepts appreciated by our allies. Currently, the United States is party to a series of international regulations governing land, sea, air, and space. A new round of international agreements could institutionalize a ban on space-based weapons and provide for verification, which many nations may well find attractive. Alone, this vision of cooperation and engagement is insufficient.

Gaining freedom of action in space over the coming decades must start with developing and implementing a comprehensive strategy. The Air Force should ensure that the nation's current space vulnerabilities do not lead to a premature and economically prohibitive strategy, or worse, spark a weapons race in space. Thus, the Air Force must tread carefully as it protects the nation's vital space interests. Four recommendations will assist the service in developing sustainable space superiority.

First, the Air Force must continue to improve American surveillance of space. A first step in correcting this deficiency was the 25 September 2010 launch of *Pathfinder*, the first satellite in a planned constellation. Known as the space-based space surveillance (SBSS) system, its mission is to improve the DoD's ability to detect and track objects in Earth orbit. To maximize its capabilities the Air Force must expedite deployment of

SBSS—or an SBSS–like constellation—and integrate it into a coherent architecture that will detect objects in both low and high Earth orbit.[19]

Second, the Air Force must guarantee access to space while achieving lower production and operating costs. While the Air Force has a rich spacefaring history, it does not have a reputation for responsive launch. Special handling requirements for lift vehicles and satellites require months or years of planning for an on-time launch. The primary space-launch vehicles in use today are evolved expendable launch vehicles (EELV)—Boeing's Delta IV family and Lockheed Martin's Atlas V family. The EELV was designed to standardize and improve space-launch operability, reduce the government's traditional involvement in launch processing, and save a projected 25 percent over legacy launch systems.[20] However, further reductions in cost are required.

Third, increased partnering with industry will also assist in reaching the goal of space superiority. The private sector has made great strides in space development over the past 20 years. SpaceX successfully launched light- and medium-lift vehicles in Falcon 1 and Falcon 9, reducing costs compared to their Boeing and Lockheed Martin rivals.[21] The Obama administration's most recent decisions on space operations, shifting spending from government projects to commercial endeavors, point to potentially dramatic changes in American space policy.[22]

Fourth, to mitigate vulnerability in space, the United States must establish greater resiliency in its satellite constellations. Space systems must become more responsive *and* less vulnerable to meet the war fighter's needs as competition in space evolves. The DoD has long relied on large, expensive satellite systems to meet its needs. The launch of the Defense Satellite Communications System (DSCS) follow-on, Wideband Global System (WGS), is an example of this good-news-bad-news story. While each WGS satellite is more capable than the entire nine-satellite DSCS constellation, the planned six-satellite WGS constellation increases US space vulnerabilities by placing greater reliance on a reduced number of satellites.[23] With space serving as a critical means of transmitting data, a loss would have a serious negative impact on cyber.

Cyber

Although the recently published AFDD 3-12, *Cyberspace Operations*, notes that "controlling the portion of cyberspace integral to our mission is a fundamental prerequisite to effective operations across the range of military

operations,"[24] cyber is not traditionally recognized as an operational military domain. With the activation of Twenty-fourth Air Force, the service sent a clear signal regarding the importance of cyberspace. The transformation of the communications and information career fields into the cyberspace operations and support career fields and the initiation of undergraduate cyberspace training also illustrated the elevated role that service leaders expect cyber capabilities to play in the future.[25] The challenge for the Air Force lies in remaining on the leading edge of advances in cyber technology.

Cyber superiority will become ever more difficult to achieve and maintain as cyber continues to act as a leveler among nations, groups, and individuals. Thus, the Air Force must advance to the leading edge of cyber.[26] Unfortunately, the number of American computer science and computer engineering graduates is shrinking while the proportion of foreign nationals receiving master's degrees and PhDs is increasing.[27] Current Air Force cyber training falls far short of providing experts capable of dealing with the threats that will come from highly trained and motivated attackers. This is a strategic concern because shortfalls in cyber capabilities undercut capabilities in other domains. The United States has rarely faced a situation in which military success depends on successful operations in a domain that it does not dominate. This is the case with cyber.

The cyberspace of 2030 will differ dramatically from that of 2010. Increases in computing power, doctrinal development, and changes in the focus of cyber attacks will make cyberspace more challenging and hostile. Cyber attacks will continue and become more relevant to military operations. In the future, cyber will evolve into a weapon of preference, replacing many of the kinetic choices in today's arsenal. The reduction in aircraft numbers and the ranges required for power projection, particularly in the Pacific, will drive cyberspace to the forefront of Air Force operations. Suppression of enemy air defenses and the ability to corrupt the software of an adversary's aircraft will become a reality, not just science fiction.

US Strategic Command (STRATCOM) is likely to find itself more deeply involved in cyberspace, expanding its operations into irregular warfare. The Air Force, while "growing its own," must also find ways to partner with academia and industry to augment its cyber force structure. These partners may not fit the mold of a traditional Airman, but their expertise will prove invaluable to accomplishing the Air Force mission.

Over the next 20 years, the cyber threat will compel the Air Force to play a leading role in defending the nation's interests. Preparing for this

future will require an unprecedented shift in the service's approach to cyber. Simply defending the network is not enough. The Air Force should undertake a more aggressive approach to developing cyber as a critical operational capability. This will require the service to undertake two principal efforts.

First, the Air Force must assume the mantle of responsibility for cyber activities as they relate to accomplishing Title 10 responsibilities. With the greatest dependence on cyber of any service, the Air Force must rely on itself for most of its cyber needs. Accomplishing this objective will require the service to operationalize cyberspace by preparing to conduct offensive as well as defensive cyber operations, develop a sound legal framework for operations, create broad interoperability, and aggressively work toward joint operations. For example, if the Air Force assumes responsibility for cyber functions directly related to its operations—some of which are performed by the National Security Agency (NSA)—the emphasis will shift from information security to operational effects.

Second, to operationalize cyberspace, the Air Force must develop a large cadre of educated experts in computer science and computer engineering (CS/CE). Because of changes in the United States' CS/CE graduate base, the Air Force faces formidable obstacles by 2030. The best people will be able to command salaries far beyond what the Air Force and the DoD offer, exacerbating this dilemma. Failure to overcome the manpower obstacle will undermine the Air Force's ability to maintain a cyber-proficient workforce and threatens the accomplishment of core Air Force missions. One way for the service to acquire the needed cyber expertise is to develop it internally, a path it is currently taking. Incentives like career specialization pay, scholarships, or bonuses can help attract and retain the best and the brightest. Whatever course the Air Force takes, it is important to remember that the interdependence of the air, space, and cyber domains makes a failure in one domain a failure in all domains.

Global Situational Awareness

The drive to 2030 is likely to include a continued drawdown of American troops permanently stationed overseas. The Air Force will likely operate primarily from CONUS locations.[28] Thus, situational awareness will become a long-distance endeavor requiring long transit and loiter times to perform surveillance and reconnaissance missions during a wide variety of

operations. The distance will also place a premium on cyber and space assets, which are likely to play an increasingly important role in building a situational awareness across far-flung regions. For example, where a drone may prove effective in uncontested airspace, cyber and space assets may be the only means of conducting surveillance and reconnaissance of peer competitors. For the United States, understanding the circumstances it faces is increasingly critical as decision makers operate in a more complex geostrategic environment.

Although the term *global situational awareness* is mentioned in AFDD 2-9, *Intelligence, Surveillance, and Reconnaissance Operations*, it is not defined in doctrine or elsewhere.[29] Thus, the development of a definition is necessary. Accordingly, global situational awareness is the understanding of the strategic, operational, and tactical environments gained through the use of space, air, sea, land, and cyber information collection systems.[30] The Air Force contribution to global situational awareness comes in the form of surveillance, reconnaissance, and analysis of data.

Since the Air Force currently has few surveillance and reconnaissance aircraft capable of covering the long distances required in a future where operations originate in the CONUS, space and cyber surveillance will play an increased role in future efforts. RPAs and autonomous platforms with longer ranges and correspondingly longer loiter times should, however, be fielded before 2030. Until their development, space and cyber assets must fill the void.[31]

Two characteristics of future space surveillance systems are critical: they must be persistent and inexpensive. The current inventory is expected to suffice well into the next decade, but the United States will require newer systems before 2030. Moreover, the concept of operationally responsive space must continue to include the ability to launch surveillance and reconnaissance payloads virtually on demand. The technical difficulties of tracking mobile targets from space also must be resolved over the next two decades.[32]

The focus on space does not mean that air-breathing platforms will become unimportant to global situational awareness. These platforms will present a different set of problems. For example, building a survivable reconnaissance platform from scratch or adapting the F-22, for example—solely for the reconnaissance mission—is not feasible in a fiscally constrained environment. The Air Force will have to make do with what is already in the inventory for the next decade or more. Given these circum-

stances, the mantra "every shooter is a sensor and every sensor is a shooter" has merit.[33]

The mission of analysis is equally important to surveillance and reconnaissance. The exploitation of reconnaissance products, particularly imagery analysis, has enjoyed a renaissance because of the creation of the distributed common ground system (DCGS) and its refinement into an agile analysis and dissemination system. Since it already operates with a reachback approach of distributed operations, the DCGS enterprise can be readily adapted to the global situational awareness concept necessary in the future.[34]

Increasing the speed of product dissemination is critical and is possible through the DCGS enterprise. However, absent the development of improved software, analysis will remain time-consuming because of the sheer volume of data and the ever-present shortage of trained analysts.[35] Sustaining a *sufficient* cadre of analysts over the next 20 years and automating many analytical tasks will assist in overcoming current deficiencies in quality and speed.[36]

Although globalization and technological advances are bringing people and nations closer together, they are making the world a more complex and expansive place for the Air Force. Nowhere will the nation feel the impact more than in situational awareness. With the Air Force traveling greater distances and facing geographically unconstrained threats, maintaining situational awareness is already becoming increasingly difficult.

To execute the situational awareness mission effectively, the Air Force's intelligence community must complete its metamorphosis into a tightly organized and dynamic force that realigns its assets for global as well as regional coverage. Implementing the following recommendations will assist in this transition.

First, overhead capabilities must be planned and executed in coordination with the National Reconnaissance Office (NRO) because surveillance is increasingly becoming a stand-off capability—making the NRO's responsibility for space asset requirements increasingly important. As part of this effort, Air Force intelligence personnel should be assigned to the NRO in sufficient numbers and with sufficient rank to influence design and implementation of programs and to provide an operational perspective from the end user. Currently, the Air Force does not always fill existing billets at the NRO. Similarly, a growing dependence on second- and third-party surveillance—since these parties are often closer to targets—will call for

exchange programs with allies and civilian partners as part of the larger effort to influence the product received by the end user.

Second, it is time to plan for a postwar (Afghanistan and Iraq) surveillance and reconnaissance structure that addresses the DCGS. Serious thought must be given to doctrine, tactics, techniques, and procedures as the DCGS' role in any future fight is reconsidered. Currently configured and manned for tactical missions, the service must shift the DCGS' focus to processing and disseminating national and allied intelligence products.

Third, the Air Force must exploit emerging automation technologies to improve data analysis so that human analysts are employed in the highest-order tasks. Accelerated development of translation software, artificial intelligence, and electronic means to process raw data—signals and electronic intelligence—is the most practical approach to managing this glut of data and should become an Air Force funding priority.

Absent significant reforms that focus on the increasing globalized nature of strategic challenges, the Air Force's contribution to national situational awareness will not reach its full potential. At a time when adversaries are chipping away at the nation's strategic advantage, failing to understand an adversary is unacceptable. Meeting this challenge can also be aided by the fourth capability—air diplomacy.

Air Diplomacy

Although the concept of air diplomacy is neither defined in doctrine nor specified as a mission of the Air Force, it is a task Airmen have performed since the early days of manned flight. Air Force history has many examples of Airmen conducting diplomatic missions, such as the Berlin airlift (24 June 1948–12 May 1949), Operation Provide Comfort/Northern Watch (1991–2003), and the ongoing training of Latin American air forces at the Inter-American Air Forces Academy (IAAFA). These examples are a small portion of the Air Force's historical contributions to American diplomacy.[37]

Currently, the Air Force conducts an array of diplomatic missions established in the Air Force Security Cooperation Strategy and many additional irregular and ad hoc diplomatic missions. While the service currently employs airpower to achieve soft-power objectives, these efforts are not optimally leveraged to the full benefit of the nation.[38] Thus, fusing the service's disparate soft-power missions into a unified air diplomacy strategy will enable the Air Force to employ its soft-power capabilities more effectively

in the pursuit of national interests. Some further clarification of the concept is necessary.

Diplomacy, broadly defined, is "the peaceful conduct of relations amongst political entities, their principals and accredited agents."[39] States conduct diplomacy to promote economic interests, protect citizens abroad, propagate culture and ideology, enhance national prestige, promote friendship, and isolate adversaries. Moreover, it is the least expensive way to exercise power in international affairs.[40] Diplomacy is one of foreign policy's two elements; the other being war. Both are means to an end rather than ends in themselves.

Air diplomacy may best be described as the nonkinetic employment of airpower in defense of national interests. While all forms of diplomacy are designed to further state interests, air diplomacy is distinguished by the means employed to promote those interests. It is important to note air diplomacy does not replace the traditional diplomacy conducted by the Department of State. It is a complementary capability provided by the Air Force. Understood in these terms, air diplomacy incorporates a broad range of Air Force soft-power capabilities into a unifying concept that highlights the service's diplomatic capabilities.

Over the next two decades air diplomacy has the potential to become increasingly important for three related reasons. First, Medicare, Medicaid, Social Security, and the national debt will consume an expanding percentage of the federal budget, which will force decision makers to reduce discretionary—principally defense—spending while remaining engaged in the international system.[41] Second, stagnant or declining defense budgets will make acquisition of new weapons less likely. People and machines capable of performing both hard- and soft-power missions will undoubtedly have the greatest appeal.[42] Third, airpower's range, speed, and flexibility will make it an attractive option for decision makers. Air diplomacy provides a range of soft-power options that, if employed before kinetic operations are necessary, may assist in preventing or resolving crises.

Simply stated, air diplomacy has the potential to be an effective approach to the defense of vital national interests, building partnerships, preventing conflict, and expanding American influence around the world. It is also a cost-effective approach that does not create the anti-American sentiment which accompanies permanent overseas bases or large troop deployments. Admittedly, it will not always succeed. But, the deliberate conduct of air diplomacy has the potential to leverage the Air Force's soft-

power capabilities more effectively before the service is called on to exercise hard power.

While the current Air Force Security Cooperation Strategy provides an excellent foundation upon which to build, an air diplomacy strategy that includes all of the service's diplomatic capabilities is necessary.[43] This is particularly important when fiscal constraints force decision makers to choose among competing priorities. Conceptually, air diplomacy also provides a construct that supports the nation's soft-power options. Devising an air diplomacy strategy is best accomplished by implementing three broad recommendations.

First, an air diplomacy strategy should focus on three central goals. It must coordinate and enhance disparate diplomatic missions; develop a proactive approach to engaging allies, neutrals, and adversaries—all within the context of each geographic commander's theater security cooperation plan; and accomplish strategic ends with existing means.

Currently, the Air Force lacks a unifying strategy capable of effectively leveraging *all* of the soft-power missions it performs. As noted previously, the Air Force Security Cooperation Strategy focuses many of the Air Force's train, advise, and assist missions into a unified strategy, but there are potential opportunities not included.[44] An air diplomacy strategy should also incorporate soft-power missions that are critical to the long-term objectives of the Air Force (access to bases, for example), but well beyond the near-term objectives of the geographic combatant commander.

Second, the Air Force should build on the foundation of existing strategic guidance, programs, plans, and approaches related to diplomatic action. This will simplify the process of creating a service strategy. With national, departmental, and service guidance found in a number of documents, it is not necessary to start from scratch when developing an air diplomacy strategy.[45] Additionally, any strategy must also create a set of guidelines for measuring the success or failure of air diplomacy.[46]

Third, bringing contributors together for the development of a strategy—accepted by key actors—is necessary. Participants should include such actors as the Department of State, the Office of the Secretary of Defense, combatant commanders, the Office of the Secretary of the Air Force for International Affairs, Air Staff components, and the major commands. If excluded from the development process, those affected by an air diplomacy strategy may not support its implementation.

The combination of hard- and soft-power capabilities outlined thus far is incomplete without the third component—military support to civil authorities (MSCA). By providing the nation the ability to persuade allies and adversaries through air diplomacy, strike adversaries through power projection, and defend the homeland through MSCA, the Air Force will provide the nation a set of critical capabilities to 2030 and beyond.

Military Support to Civil Authorities

Military support to civil authorities is becoming increasingly important because of the proliferation of nuclear weapons technology, advanced missile technology, and offensive cyber capabilities. Current capabilities for disaster response are also insufficient to meet demands. This combination of variables is certain to make MSCA a critical capability for the Air Force well into the future. Admittedly, a natural disaster is more likely than a major terror attack, but in either case the Air Force and the Air National Guard (ANG) can expect to play major roles in providing the US Northern Command (NORTHCOM) a range of capabilities to mitigate the effects of a catastrophic event.[47]

AFDD 2-10, *Homeland Operations*, cautions that USAF forces "are only made available when not required by other military operations."[48] Air Force Instruction (AFI) 10-802, *Military Support to Civil Authorities*, states that ANG forces (on state orders, not in federal service) have the "primary responsibility for providing military assistance to state and local governments in civil emergencies."[49] In short, the ANG not only can respond well ahead of any federal military effort, but is also expected to do so by Air Force instruction.[50] Short of a man-made catastrophe involving chemical, biological, radiological, or nuclear materials, it is unlikely that active duty resources will be called upon. Nevertheless, if a disaster rises to the level of a catastrophe, state and local resources may be overwhelmed. Governors are likely to ask for federal assistance, which may or may not be readily available because of Air Force decisions.[51]

The challenging economic environment that will persist well into the future is certain to amplify the importance of Air Force and ANG military support to civil authorities. If the nation's interests continue to shift and technological innovations bring America's adversaries closer to its shores, the American public will expect the military to focus on missions such as homeland defense and disaster relief. For the Air Force and the ANG, this

means providing MSCA capabilities in three areas: situational awareness, medical support, and airlift.[52]

Given the Air Force's role in shaping the ANG through its organize, train, and equip responsibilities, it is vital for service leaders to elevate MSCA to a critical capability.[53] Dual designed operational capability (DOC) statements, particularly for the ANG, will assist in establishing the role of individual units in MSCA and wartime. In other words, the Air Force and ANG roles in providing MSCA are intertwined and inseparable. Thus, any discussion of the ANG role in MSCA is also a discussion of the Air Force role.

The Air Force and ANG can contribute to building a more resilient domestic response capability. However, there is significant reason for concern. Today's total force approach may prove inadequate in the event of a major disaster in the United States—with speed of response the principal concern.[54] Thus, a renewed focus on MSCA will better serve the nation. Given the interconnected nature of the MSCA mission, three recommendations will enable the Air Force and the ANG to improve disaster response while maneuvering through a difficult legal, political, and command and control environment.

First, airlift aircraft should form the bulk of the Air National Guard's future unit structure. First-response airlift is a key enabler and will likely come from the ANG. Thus, a focus on airlift will enable the ANG to not only provide military support to civil authorities, but to perform a valuable wartime mission as well. Embedded within each ANG airlift unit must be aerial port capabilities to provide staging expertise for follow-on operations.

As part of a focus on airlift, ANG airlift units should include medical support units, which are the most critical and long-lasting components of MSCA. They are often required before anything else and must continue long after any disaster. As the Air Force's "first responder," the ANG should be postured to fill this quick-response role.

Second, beddown of all future ANG airlift units should be aligned among the 10 Federal Emergency Management Agency (FEMA) regions. Aligning ANG airlift units among FEMA regions will allow these units to exercise with state and local first responders in disaster scenarios and establish strong relationships before a disaster occurs.[55]

Third, ANG imagery analysts should become the primary source of support, advice, liaison, and imagery interpretation for state and local

officials within each FEMA region. They should be an integral part of future MSCA exercises and remain on call for domestic disaster support. Gaining situational awareness of a disaster's dimensions is a crucial step in dealing with it. As part of this effort to improve situational awareness for first responders, distributed common ground system stations staffed by ANG analysts should be used to provide real-time imagery support in the event of a disaster, and their DOC statements should be amended to add MSCA. Codifying this mission will allow ANG units to exercise with local and state disaster entities as well as provide a framework for oversight, funding, and inspection.

By implementing these recommendations, the Air Force active and ANG units remain poised to effectively respond in the event of a disaster. Defense of the homeland is, at its most fundamental, the very reason for maintaining a military.

Conclusion

As the Air Force looks toward a future that will be characterized by turbulence and rapid change, service leaders must make a number of difficult decisions well in advance of an eventual need. Confronted by uncertainty, flat defense budgets, and threats at the high and low ends of the conflict spectrum, current decisions that will shape the future of the Air Force must account for an increasingly complex array of variables. Success in this environment is not assured and should not be taken for granted. By suggesting the service focus on five critical capabilities (power projection; freedom of action in air, space, and cyberspace; global situational awareness; air diplomacy; and military support to civil authorities), this article seeks to both clarify the areas where the service should focus its time, resources, and strategic thought. It also highlights a persistent challenge. It is the responsibility of the Air Force to articulate a clear rationale for investing in airpower. Strategy development enables this fundamental task. SSQ

Notes

1. John Shaud, *Air Force Strategy Study 2020–2030* (Maxwell AFB, AL: Air University Press, 2010). Appendix A provides a discussion of national interests. Appendix B provides an environmental scan (trends) and a discussion of the research methodology that was used. Appendix C includes the four scenarios (peer competitor, rising or resurgent power, failed state, and jihadist insurgency).

2. Morton Abramowitz and Stephen Bosworth, "Adjusting to the New Asia," *Foreign Affairs* 82, no. 4 (July–August, 2003), 119–31; Jonathan Pollack, "US–Asia Pacific Strategy in the Obama Administration," in *American Foreign Policy: Regional Perspectives* (Newport, RI: Naval War College Press, 2009), 101–10; and Evan Medeiros, "The New Security Drama in East Asia: The Response of US Allies and Security Partners to China's Rise," in *American Foreign Policy*, 111–24.

3. Mark Gunzinger and Jim Thomas, *The 2010 Quadrennial Defense Review: An Initial Assessment*, Center for Strategic and Budgetary Analysis Backgrounder, February 2010, http://www.csbaonline.org/4Publications/PubLibrary/B.20100201.The_2010_QDR_An_In/B.20100201.The_2010_QDR_An_In.pdf.

4. Andrew Krepinevich, Barry Watts, and Robert Work, *Meeting the Anti-Access and Area-Denial Challenge* (Washington: Center for Strategic and Budgetary Analysis, 2003), http://www.csbaonline.org/4Publications/Archive/R.20030520.Meeting_the_Anti-A/R.20030520.Meeting_the_Anti-A.pdf; and Sam J. Tangredi, "The Future Security Environment 2001–2025: Toward a Consensus," in *American Defense Policy*, ed. Paul Bolt et al. (Baltimore: Johns Hopkins University Press, 2005), 48–65.

5. Secretary of Defense Robert Gates, *Quadrennial Defense Review Report* (Washington: DoD, February 2010), vi, http://www.defense.gov/qdr/images/QDR_as_of_12Feb10_1000.pdf; and Andrew S. Erickson and David D. Yang, "On the Verge of a Game-Changer," *Proceedings* 135, no. 5 (May 2009): 26–32, http://www.usni.org/magazines/proceedings/2009-05/verge-game-changer.

6. A recent Office of the Secretary of Defense (OSD) report to Congress on Chinese military capabilities assessed China's antiaccess and area-denial capabilities as moving toward building a credible force that could threaten operations and forces as far away as Guam. See OSD, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2010* (Washington: OSD, 2010), 29–39, http://www.defense.gov/pubs/pdfs/2010_CMPR_Final.pdf.

7. Krepinevich, Watts, and Work, *Meeting the Anti-Access and Area Denial Challenge*, 20.

8. A 2005 report noted, "US military strength is built on a foundation of technological superiority that grew from a position of global leadership in relevant technologies and innovative capabilities. That leadership position is no longer assured. The synergistic forces of globalization and commercialization of science and technology are providing current and future adversaries with access to advanced technologies as well as the expertise needed to exploit those technologies." Committee on Defense Intelligence Agency Technology Forecasts and Reviews, Division on Engineering and Physical Sciences, *Avoiding Surprise in an Era of Global Technology Advances* (Washington, DC: National Academies Press, 2005), 1. More recently, another defense analyst observed, "It is important here to note that as the pace of innovation may be slowing for the United States, American competitors may be catching up. For example, in coming years China could gain the ability to use large numbers of precision submunitions launched from maneuverable ballistic missile reentry vehicles. These could, in theory, make it quite impractical to use airfields lacking hardened shelters; and even those with shelters could have their runways threatened." Michael E. O'Hanlon, *The Science of War* (Princeton, NJ: Princeton University Press, 2009), 184.

9. John Shaud, *In Service to the Nation: Air Force Research Institute Strategic Concept for 2018–2023* (Maxwell AFB, AL: Air University Press, 2008), 7.

10. See, for example, Robyn Read, "Effects-Based Airpower for Small Wars: Iraq after Major Combat," *Air and Space Power Journal* 14, no. 1 (Spring 2005): 103–12, http://www.airpower.maxwell.af.mil/airchronicles/apj/apj05/spr05/read.html.

11. Michèle Flournoy and Shawn Brimley, "The Contested Commons," *Proceedings* 135, no. 7 (July 2009): 3.

12. Werner J. A. Dahm (chief scientist, USAF), *Report on Technology Horizons: A Vision for Air Force Science and Technology during 2010–2030*, vol. 1 (Washington: Department of the Air Force, 15 May 2010), 6.

13. Robbin Laird, "Combat Air Power: The Need for a New Path: A Conversation with General Corley about the Future of Air Power," *Second Line of Defense*, August 2010, http://www.sldinfo.com/?p=11608.

14. Dahm, *Report on Technology Horizons*, 6, 41.

15. Ibid., 60.

16. Government Accountability Office (GAO), *Joint Strike Fighter: Additional Costs and Delays Risk Not Meeting Warfighter Requirements on Time* (Washington: GAO, 2010).

17. The White House, *National Space Policy of the United States of America* (Washington: White House, 28 June 2010), 3.

18. John Oneal and Bruce Russett, *Triangulating Peace* (New York: W. W. Norton, 2001).

19. 30th Space Wing Public Affairs, "Vandenberg Launches Minotaur IV," 26 September 2010, http://www.vandenberg.af.mil/news/story.asp?id=123223753.

20. 30th Space Wing Public Affairs, "Evolved Expendable Launch Vehicle (EELV)," http://www.vandenberg.af.mil/library/factsheets/factsheet.asp?id=5207.

21. Siemens PLM Software, "Case Study: SpaceX Delivers Outer Space at Bargain Rates," 15 September 2010, http://www.plm.automation.siemens.com/en_us/about_us/success/case_study.cfm?Component=30328&ComponentTemplate=1481.

22. Kenneth Chang, "Obama Calls for End to NASA's Moon Program," *New York Times*, 1 February 2010.

23. Ed White and Andy Roake, Air Force Space Command Public Affairs, "First Wideband Global SATCOM Satellite Goes Operational," 29 April 2008, http://www.stratcom.mil/news/article/38/first_wideband_global_satcom_satellite_goes_operational.

24. AFDD 3-12, *Cyberspace Operations*, 15 July 2010, http://www.dhs.gov/files/cybersecurity.shtm.

25. David S. Alberts et al., *Understanding Information Age Warfare* (Washington: Command and Control Research Program (CCRP) Publication Series, 2001); Alberts and Daniel S. Papp, eds., *Information Age Anthology*, vol. 1, *The Nature of the Information Age* (Washington: CCRP Publication Series, 2001); Alberts, J. J. Garstka, and F. P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority* (Washington: National Defense University Press, 1999); and Alberts, *Information Age Transformation: Getting to a 21st Century Military* (Washington: CCRP Publication Series, 2003).

26. Ibid.

27. Computing Research Association, *Taulbee Survey of US Computer Science and Computer Engineering Graduate Programs*, (1974–2009).

28. Stephen J. Hagel, Adam B. Lowther, and Chad L. Dacus, *The Future of Global US Air Force Basing 2010–2040* (Maxwell AFB, AL: Air Force Research Institute, 2010), 60.

29. AFDD 2-9, *Intelligence, Surveillance, and Reconnaissance Operations*, 17 July 2007, 24.

30. Jeffrey Horne, "Transforming National Space Security: Enabling DoD and Intelligence Community Defensive Space Control Collaboration," *High Frontiers* 4, no. 4 (August 2008): 15–16; DHS, "DoD, DHS and DOJ Co-Sponsor a Critical Incident Preparedness Conference for First Responders," *NIPP [National Infrastructure Protection Plan] Newsletter* 38 (November 2008), 3; and Maryann Lawlor, "Covering the Six for Homeland Joint Operations," *SIGNAL-online*, May 2009.

31. Add airships to the list of long-loiter assets in development for surveillance missions. Development is expected to take years beyond the first prototypes. David Pearson, "Airships Receive Lift from New Technology," *Wall Street Journal*, 27 August 2010, B-8. Moreover, those systems that are serving so well in the CENTCOM area of responsibility (AOR) can form the basis for a CONUS–based homeland defense/homeland security program along our borders in the outyears and for use in disaster response as well.

32. In an interview with staff members of the Air Combat Command (ACC) Directorates of Intelligence (A2), Air and Space Operations (A3), Plans and Programs (A5), and Requirements (A8) in June 2010, several individuals commented on the inability of satellite imagery to react to even the slightest modifications of targets, referring to how "a little aluminum foil" could change the shape of an object on the ground and "mess up" a satellite's ability to discriminate targets via its moving target indicator. Unattributed interview by the author, Air Combat Command, Langley AFB, VA, 22 June 2010. (All interviews were conducted in confidentiality, and the names of interviewees are withheld by mutual agreement.)

33. Although this expression has been used for a number of years, it most recently appeared in Department of the Air Force, *Lead Turning the Future: The Vision and Strategy for United States Air Force Intelligence, Surveillance and Reconnaissance* (Washington: Headquarters USAF, 2010), 19.

34. Air Force ISR Agency, "Air Force Distributed Common Ground System," *AF.mil*, 31 August 2009, http://www.af.mil/information/factsheets/factsheet.asp?id=15433.

35. At present, the entire DCGS enterprise is being criticized by the Army for not having a sense of the fight since it operates from afar. To that end, the DCGS community is preparing an expeditionary-like unit to process data in-theater to more quickly satisfy commanders' needs and to get a sense of the fight. Some interviewees amplified their remarks, stating that due to long lag time in stateside processing, Marine users in the AOR have stated that if the data is over three days old, they do not want it. ACC staff members, interview.

36. Jim Hodges, "The Get-Well Intel Plan," *C4ISR Journal*, 1 January 2010, http://www.c4isrjournal.com/story.php?F=4411944. In the interim, Air National Guard personnel and Air Force Reserve individual mobilization augmentees (IMA) have performed thousands of days of active duty per year to support the effort.

37. Roger G. Miller, *To Save a City: The Berlin Airlift, 1948–1949* (Washington: Air Force History and Museums Program, 1998). See also "Inter-American Air Forces Academy," Lackland AFB website, http://www.lackland.af.mil/IAAFA; and Michael Knights, *Cradle of Conflict: Iraq and the Birth of Modern U.S. Military Power* (Annapolis, MD: Naval Institute Press, 2005), 217–30.

38. See Jennifer D. P. Moroney et al., *International Cooperation with Partner Air Forces* (Washington: Rand Publishing, 2009), 9; Gordon England, *Building Partnership Capacity: QDR Execution Roadmap* (Washington: DoD, 2006); and Bruce Lemkin, *Global Partnership Strategy* (Washington: DAF, 2008).

39. Keith Hamilton and Richard Langhorne, *The Practice of Diplomacy: Its Evolution, Theory, and Administration* (London: Routledge, 1995), 1. Hedley Bull offers a similar definition, suggesting that diplomacy is "the conduct of relations between states and other entities with standing in world politics by official agents and by peaceful means." Bull, *The Anarchical Society: A Study of Order in World Politics*, 3rd ed. (New York: Columbia University Press, 2002), 156.

40. A. F. K. Organski, *World Politics* (New York: Alfred A. Knopf, 1968), 401.

41. "Obama's Budget Ignores Entitlement Crisis," Heritage Foundation, accessed 5 February 2010, http://www.heritage.org/research/features/budgetchartbook/obama-scenario.aspx; Mary Williams Walsh, "Social Security to See Payout Exceed Pay-in This Year," *New York Times*, 24 March 2010, http://www.nytimes.com/2010/03/25/business/economy/25social.html; Stephen

Ohlemacher, "1 Out of 6 Americans Depend on Programs for Poor," *Seattle Times*, 26 February 2007, http://seattletimes.nwsource.com/html/nationworld/2003589315_welfare26.html; and Douglas Elmdorf (director, Congressional Budget Office), to Nancy Pelosi (Speaker of the US House of Representatives), letter, 20 March 2010, http://www.cbo.gov/ftpdocs/113xx/doc11379/AmendReconProp.pdf.

42. Adam Talaber and Daniel Frisk, *Long-Term Implications of the Fiscal Year 2010 Defense Budget* (Washington: Congressional Budget Office, 2010), 8.

43. USAF, *Global Partnership Strategy: Building Partnerships for the 21st Century* (Washington: DAF, 2008).

44. Ibid., 2.

45. Robert Gates, *Department of Defense Report on Strategic Communication* (Washington: OSD, 2009).

46. Jennifer Moroney, *Building an Assessment Framework for U.S. Air Force Building Partnership Programs* (Washington: RAND, 2010).

47. Stephen Flynn, "U.S. Not Prepared for the Next 'Big One'," *CNN.com*, 20 February 2007, http://www.cnn.com/2007/US/02/20/flynn.commentary/index.html.

48. AFDD 2-10, *Homeland Operations*, 21 March 2006, 5. This is discussed further in DoD Directive (DODD) 3025.1, *Military Support to Civil Authorities*, 15 January 1993.

49. AFI 10-802, *Military Support to Civil Authorities*, 19 April 2002, par. 4.3.4.

50. This echoes similar wording in JP 3-26, *Homeland Security*, 2 August 2005, and in DODD 3025.1, *Military Support to Civil Authorities*.

51. Wayne H. Nelson and David Arday, "Medical Aspects of Disaster Preparedness and Response—A System Overview of Civil and Military Resources and New Potential," *Joint Center for Operational Analysis (JCOA) Journal* 9, no. 2 (June 2007): 11. See also Justin Rood, "Medical Catastrophe," *Government Executive*, 1 November 2005, http://www.govexec.com/features/1105-01/1105-01s1.htm. For example, catastrophes could be earthquakes of a 6.0 magnitude or higher, tsunamis, or volcanic eruptions.

52. AFDD 2-10 lists eight examples of Air Force capabilities (along with a laundry list of "Potential Defense Support of Civil Authority Missions" in fig. 3.1) which are based on previous missions. AFDD 2-10, *Homeland Operations*, 27. An Army National Guard homeland defense white paper lists "Top 10 Essential Homeland Defense Capabilities," seven of which have an obvious air component mission. US Army National Guard, "September 11th, 2001, Hurricane Katrina, and Beyond," 11 October 2005, 11, http://www.arng.army.mil/News/publications/Publications/HLD%20White%20Paper_11OCT05_Final_Version.pdf). See also *The Federal Preparedness Report* (Washington: DHS, January 2009), table 2, 100, for a listing of 13 DoD asset contributions, the majority of which are suitable for Air Force accomplishment, http://www.iaem.com/committees/governmentaffairs/documents/FPR-Jan2009.pdf; and *Joint Center for Operational Analysis Journal* 9, no. 2 (June 2007): table 4, 17. For a list of seven emergency measures that the federal government can unilaterally provide, see the American Bar Association (ABA) Standing Committee on Law and National Security, *Hurricane Katrina Task Force Subcommittee Report* (Washington: ABA, February 2006), 5, http://www.abanet.org/adminlaw/KatrinaReport.pdf.

53. J. Emery Midyette Jr., "Resource and Structure of States' National Guard," *Joint Center for Operational Analysis Quarterly Bulletin* 8, no. 2 (June 2006): 33, 37, https://transnet.act.nato.int/WISE/test/LessonsLea/JCOALL/JCOABullet6/file/_WFS/JCOA%20Katrina.pdf.

54. On average, local and state authorities handle about 25 "disasters" per year, only about 15 of which result in 40 or more casualties. Nelson and Arday, "Medical Aspects of Disaster Preparedness and Response," 13. Floods, mudslides, forest fires, and similar disasters are usually

localized, do not cause calamitous loss of life or property, and do not disrupt interstate commerce or impact national security. Here is where the National Guard is most likely to respond within their states or in concert with other Guard units under emergency military assistance compacts (EMAC). As the commander in chief within their states, governors can recall National Guard personnel in state active duty (SAD) status or under 10 USC Title 32. In both cases, Guard personnel are under the command and control of the governor, as exercised through the state's adjutant general. Moreover, Guard forces in SAD status or under Title 32 status can restore public order using police powers that federal forces do not have under the Posse Comitatus Act. If federal (Title 10) forces are needed, an elaborate process must take place to get them on the ground. According to the White House analysis of the military response to Hurricane Katrina, DoD assets were dispatched only after an approval process requiring *21* separate steps. Lag time between the request and federal "boots on the ground" was measured in days, not hours. "Integrated Use of Military Capabilities" in *The Federal Response to Hurricane Katrina: Lessons Learned* (Washington: White House, February 2006), chap. 5, 5, http://georgewbush-whitehouse.archives.gov/reports/katrina-lessons-learned/chapter5.html.

55. For a detailed review of how to base ANG airlift aircraft for domestic support, see John Conway, "Beddown Options for Air National Guard C-27J Aircraft: Supporting Domestic Response," *Air and Space Power Journal* 24, no. 2 (Summer 2010): 35–44, http://www.airpower.maxwell.af.mil/airchronicles/apj/apj10/sum10/06conway.html.

Rise of a Cybered Westphalian Age

Chris C. Demchak
Peter Dombrowski

No frontier lasts forever, and no freely occupied global commons extends endlessly where human societies are involved. Sooner or later, good fences are erected to make good neighbors, and so it must be with cyberspace. Today we are seeing the beginnings of the border-making process across the world's nations. From the Chinese intent to create their own controlled internal Internet, to increasingly controlled access to the Internet in less-democratic states, to the rise of Internet filters and rules in Western democracies, states are establishing the bounds of their sovereign control in the virtual world in the name of security and economic sustainability. The topology of the Internet, like the prairie of the 1800s' American Midwest is about to be changed forever—rationally, conflictually, or collaterally—by the decisions of states.

In 2010 the crossing of the Rubicon into the age of cybered conflict[1] occurred with a surprisingly sophisticated, precisely targeted, and undoubtedly expensively produced worm in large industrial control systems. Its name was Stuxnet. As a malicious piece of software, it came as a surprise despite having floated around a year doing nothing but stealthily copying itself. The worm's target was the program controlling centrifuges in Iranian nuclear reprocessing plants.[2] Spread by infected USB thumb drives and the software in printer spoolers, it bypassed the Internet security controls in place against hackers and did not act maliciously until finding

---

Dr. Chris C. Demchak, a former Army Reserve officer, received her PhD in political science from UC Berkeley and holds an MPA in economic development from Princeton and an MA in energy engineering from Berkeley. She has published articles on comparative security, cyberspace, organizations, and large-scale systems surprise and three books: *Military Organizations, Complex Machines*; *Designing Resilience*; and (forthcoming) *Wars of Disruption and Resilience*: *Cybered Conflict, Power, and National Security*.

Dr. Peter Dombrowski is a professor of strategy at the Naval War College and chair of the Strategic Research Department. Previous positions include director of the Naval War College Press, editor of the *Naval War College Review*, co-editor of *International Studies Quarterly*, associate professor of political science at Iowa State University, and defense analyst at ANSER, Inc. He has authored over 45 articles, monographs, book chapters, and government reports and is co-editor of *Balance Sheet: The Iraq War and U.S. National Security* (Stanford University Press, 2009).

the precise computer DNA of Iranian nuclear reactors as Stuxnet's designers intended. While the worm infiltrated a wide variety of protections and Windows operating systems, the sophisticated Stuxnet authors demonstrated a new level of threat to cyber security. Despite early denials, the Iranian nuclear community ultimately admitted its plants were infected and its centrifuges unstable.

Stuxnet capped a two-year period in which the scope and complexity of national security challenges posed by cyberspace created a new level of insecurity.[3] From 2008 onward, a string of unsettling discoveries of massive theft of national data appeared via backdoors into otherwise secure national-level systems (e.g., GhostNet). Widespread stealthy infection of national systems occurred through sophisticated programs waiting to be connected to hidden remote servers, such as the Confiker worm and the wholesale copying of critical industrial technological advances by China. The age of vandals and burglars in cyberspace moved to the next level, resembling organized cyber mercenaries, cross-national pirates, and the undermining of nation-states on a massive cyber scale.[4]

Until Stuxnet, however, it was not entirely clear if all the access points, malware, and rampant penetrations would lead to serious strategic harm. The consensus among states changed after Stuxnet. If such malicious software can take down whole energy systems at once, states have no choice but to respond if they are to protect their own governmental and military operations and uphold their responsibility to protect citizens and corporations.[5] The Stuxnet method and its success thus changed the notion of vulnerability across increasingly internetted societies and critical infrastructures. The days of cyber spying through software backdoors or betrayals by trusted insiders, vandalism, or even theft had suddenly evolved into the demonstrated ability to deliver a potentially killing blow without being anywhere near the target. Forcing nuclear centrifuges to oscillate out of control from an unknown and remote location suggests that future innovations might be able to destroy or disrupt other critical infrastructures upon which modern societies depend. As proof of concept as well as a model to be copied, the Stuxnet worm offers the possibility of distant enemies spending hundreds of staff hours and expertise to insert such applications throughout the nation—from oil pipelines to dam turbines to nuclear and fossil fuel energy plants to any other large-scale critical service controlled by computers. As the designers of Stuxnet demonstrated, being disconnected from the Internet will never again be a guarantee of security.[6]

If any part of the plant, service, aircraft, or system is internally connected or if any electronic devices connect to the system from the outside, even if the device must be hand-carried, the system is vulnerable.

Stuxnet is an exquisite example of the advantages afforded attackers in the current global cyberspace. Attackers freely choose the scale of their organization, the proximity of their targets, and the precision of their target group, all with near impunity. They may take all the time they need in capitalizing on these advantages and in using the Internet itself to collect more data on the intended targets. The ease of relatively risk-free conflict between adversaries within the global web is so apparent even bot net gangs of criminals controlling secretly hacked personal computers fight among themselves technologically, often seeking to destroy and replace the other's malicious software. As shown by the denial of government and banking service in Estonia in 2007, wholesale assaults across physical borders can be deployed from one state to another by "patriotic hackers," while the originating state claims ignorance and inability to stop the assault.[7] By 2008 alone, the daily attacks on simply the US ".gov" or ".mil" websites numbered in the millions.[8] Over the course of 2009, an unprecedented 75 percent of global companies across 27 countries were the victims of cyber attack, with the average reported loss of $2 million.[9]

Today, protective measures in modern democratic states are often insufficient to repel the daily onslaught of attacks by state and nonstate actors, and the situation is worsening. Stuxnet's success ensured the rising perception of an all-source 24/7/360-degree national-level threat. In the future, a "son of Stuxnet" variant could also float for some time, seemingly harmless and unnoticed until triggered by a particular date, end-use, Internet signal, or an encounter with a specific kind of computer or program. At once, millions of computers might fail, suddenly try to send destroy commands to countless others, or even worse, suddenly replace true data with false in anything from aircraft to mass financial transactions. Even China recognizes an internal threat from its own vigorous development of cybered hacking talent inside the nation. While the intent had been to use the skills outwardly in "patriotic hacking," despite severe sanctions against hacking Chinese citizens, now Chinese authorities have to contend with their own very real internal cybered threats.[10] States under such constant barrage cannot help but respond.

All states, in one way or another, will reach out to control what they fear from the Internet—the lack of sovereign control over what comes through

their borders. Thus the transformation from frontier to regulated substrate across cyberspace has begun. While it is not recognized as such nor publicly endorsed by most democratic leaders, a cyberspace regulating process is happening, building the initial blocks of emergent national virtual fences. A new "cybered Westphalian age" is slowly emerging as state leaders organize to protect their citizens and economies individually and unwittingly initiate the path to borders in cyberspace. Not only are the major powers of China and the United States already demonstrating key elements of emerging cybered territorial sovereignty, other nations are quickly beginning to show similar trends. From India to Sweden, nations are demanding control over what happens electronically in their territory, even if it is to or from the computers of their citizens.

This process may be meandering, but we argue it was inevitable, given the international system of states and consistent with the history of state formation and consolidation. As cyberspace is profoundly man-made, no impossible barriers hinder the growth of national borders in cyberspace. They are possible technologically, comfortable psychologically, and manageable systemically and politically. Small steps in securing against threats will lead to further steps over time and, especially, in response to discoveries such as Stuxnet or its derivatives in the future.

In the process of border development, the singular marker of a new age of sovereignty and cybered conflict will come to be a normal part of the modern state's capacities: the national cyber commands or their security equivalents at the national level. To assure national safety in cyberspace, large, vulnerable states like the United States and China must anticipate and disrupt attacks far forward as well as repel a wide variety of threats. Otherwise, the mass attacks may spread too fast for effective defense. Just as militaries still exist in the modern age of mass weapons, they or their functional equivalents will also be sent to guard key national points in cyberspace. In so doing, they deepen national borders. This article argues Stuxnet marks the official beginning of a new cyber Westphalian world of virtual borders and national cyber commands as normal elements of modern cybered governments. Finally, we have seen these kinds of phenomena before in the old Westphalian world. Already, theories, international rules, institutions, and experiences exist to guide us as the new age fully matures.

The "Westphalian" Process

The Stuxnet worm marks a turning point into a new cybered conflict age in which states need to define territorial spaces of safety to reassure their citizens' safety and economic well-being. When it is widely accepted that critical systems can no longer be trusted if they are open to the web, political leaders will demand ways to eliminate the threats from entering their territory. The cybered conflict age has begun, and it is natural for those hostile to any particular group to include cyber at key points in their plans, including debilitating entire systems. Equally expected, leaders of the threatened group will have to consider what responses keep critical functions secure. From water holes in the desert to river passages in the forest to mountain passes to central controlling nodes in the global web, conflict parties inevitably seek the critical gateways of the opposition to obtain advantage.

Frontiers are places of conflict between groups, historically lightly and poorly governed, less populated, and risky—places where value is extracted for little cost. When a frontier starts to become a commons, productivity for all is imperiled by the grab-and-go nature of those using it. Those dependent on the frontier tend to form organizations to control their claim. Modern democracies are in essence complex aggregates of large-scale organizations. Their leaders routinely reach out to absorb uncertainties to control them, if possible, or push them away.[11] The rising perception of a national-level threat means that all states, in one way or another, will reach out to control what they fear from the Internet—its frontier nature and the lack of sovereign control over what comes into their area of responsibility.

No freely occupied commons extends endlessly nor lasts forever where rising rapacious human populations are involved. It is normal for political leaders seeking relief from the interaction edges with other cultures or possible threats to look at reinforcing or installing borders. Being able to establish sovereign control is one hallmark of a functioning state. This need is true whether the border is enforced by passports for people, customs inspections for goods, or two-way filters for meta-tagged electronic bits. When states cannot protect their economic engines of growth and sustainability, the capacity of the state falls into question by those who control the resources under threat.[12]

Man's search for security has led to the formation of "fortress and badland" distinctions that marked territory for resource ownership for centuries, but

until the 1648 Treaties of Münster and Osnabrücke (understood together as the Peace of Westphalia), borders did not stabilize over many generations. In this particular case, however, the Peace of Westphalia not only ended the Thirty Years' War in Europe but also heralded the emergence of the modern interstate system. After the Westphalian peace, the nation-state became the dominant form of social organization. As a result, leading states of the period helped codify and set about more or less enforcing a collectively agreed upon set of rules, institutions, and norms by which they interacted with each other in international society.[13]

Particularly useful for international stability was the effect of the treaties in creating conditions supporting the gradual hardening of borders between and among states, more or less, over the next 362 years. This process of settling on boundaries due to the mutual adjustments among states produced a concept of national territoriality that states could legitimately claim, and they could defend that territory against outside aggressors in just wars. With the rise of a general presumption of territoriality recognized by other external political leaders, modern states were able to stabilize internally and grow economically within those established, increasingly fixed borders.

Westphalia provided a demonstration or a proof of concept. Over time, the more established a state became and the fewer ungoverned internal areas or frontiers it allowed to continue, the stronger and less existentially vulnerable the nascent state became.[14] The significance of the Westphalian process for this article and its general argument is that the efforts of the modern state to cope with the emergence of the cybersphere is in many respects similar to the processes by which states became the dominant form of social organization within the international system. The ability of the state to provide stability and security within the increasingly unchallenged borders was necessary to internal development of social and economic progress. Without a form of Westphalian borders, conflicts previously at the boundaries easily spill over in both directions from opportunistic resource appropriations by actors within and without. The wide variety of authorities, powers, and capabilities over the last 400 years accruing to the modern state become difficult to employ, redirect, or even limit. Just as the ability of modern bureaucratic states to corral resources productively drove other less successful organization forms from the scene internationally, their ability to provide internal certainty in their domestic territory gradually

came to define what is today known as civil society in the Westernized world.[15]

Today the uncertainties, predatory and productive opportunism, legal and illegal resource conflicts, and changes to economic and social expectations reach directly into the domestic structures of the modern state. Just as before the Peace of Westphalia and its recognition of the systemic economic threats of insecurity within societies, states are beginning to grapple with the difficulties inherent in incorporating a new set of technologies into their citizens' community and individual interactions. In particular, the cybersphere has challenged the security of individuals and states themselves in ordinary systems considered essential to the critical functions of society. Increasingly, citizens are at the frontlines of the existential fight over stability in the wider society, and the responses from modern states have only now begun to crystallize.

The struggle to move these conflicts from the existential realm directly harming citizens to some more organized field of dispute has begun at least in discussions among allies and in international communities, but the process has been meandering.[16] Initially surprised by the reach of the predatory behaviors made possible by cyberspace's unfettered global reach, democratic governments have been slow to reinforce their monopoly of violence over external threats entering their nations and harming citizens. Laws emerged over the early 2000s focused on the internal symptoms rather than the external sources of the uncertainties, many focused on the individual citizen or commercial Internet service providers (ISP). For example, in the United States, financial liability to the individual defrauded online in credit card usage limited the amount the citizen would lose.[17] In contrast, German law makes individual citizens responsible if they do not stop their personal computers from being taken over and used in massive spam or denial-of-service attacks.[18] Australia, however, enforces rules on the ISPs to keep the flow of malware to a minimum.[19]

Despite these efforts, organizations and governments have found their presence in cyberspace vulnerable to attempts to extract information, prevent access, and even to disable as happened with Stuxnet. In March 2010, a US cyber security report stated the monthly number of attacks on the US Congress and government agencies had reached 1.6 billion, largely from outside US borders.[20] Governments, like the signatories to the Peace of Westphalia, are increasingly aware of the potential losses if hostile, curious, or just rapacious outside actors are able to reach easily and deeply inside

their societies, into critical assets of families, banks, townships, airlines, or any of the myriad of critical systems sustaining the society. "It appears we can no longer see the Internet as a friendly shared resource and that strict boundaries will have to be put in place," said Bert Hubert, founder of Dutch-based software provider PowerDNS.com.[21] States, especially large, often cyber-targeted nations like the United States, are recognizing the need to respond. Their efforts to control are accumulating across the organizational and technological capabilities. The modern state intends to put in place a buffer, a bulwark, a way to buy the nation time to respond if attacked. In short, they are iterating toward national borders in cyberspace to relieve the pressure of the barrage of assaults.

Practical Reinforcement—Borders Decrease the Ease of Cybered Offense

Beyond the return to interstate protocols that are well understood, there is a practical aspect to cyber borders—they make it more difficult to cause harm. Making it necessary to get around borders physically forces larger organizations of people to arrange a physical entry to each nation under attack. Forcing attackers and criminals to move people rather than bytes means higher operational barriers to entry: more costs, more coordination efforts, and many more opportunities for any of these efforts to be noticed by national security monitoring organizations.[22] The border hurdles also can slow the pace of regrouping from failures or redirecting to capitalize on new information, as well as coordinating simultaneous target groups across borders.

Increasing the organizational difficulties for attackers also increases the loyalty challenge for bad actor organizations trying to control human agents at distance rather than merely reprogramming pawned computer networks. The job of attacking civil societies increases enormously when information must be verified in situ by informants who may or may not be trustworthy dispersed across monitored virtual borders. Borders reduce the advantages of scale, proximity, and precision an attacker has in pitching offensive surprises and levels the playing field for the defending societies. Some mass attacks that are possible today may, with borders, simply become impossible unless the organization is able to physically move large numbers of humans into each targeted country and coordinate rapidly around national borders or collaborating regional institutions. Borders

raise skill, social, resource, and distance barriers for the vast majority of today's hackers and would-be attackers who lack exceptionally advanced skills.

Virtual Borders—Feasible, Comfortable, and Manageable

The slow development of a Westphalian-style accord parsing cybered sovereignty has every chance to proceed and eventually succeed. There are few natural dampeners to a neo-Westphalian process in the digital era. A cybered national border is technologically possible, psychologically comfortable, and systemically and politically manageable. Increasingly, the exceptionally skilled technologists are arguing for separation of critical systems to protect them from Internet predators and hostile actors. As a result, even if policymakers in each nation are inclined normatively to keep a fully open Internet, they will have few technical arguments to use in maintaining that position. Furthermore, borders are psychologically normal for citizens focused on continuing their access to Internet services safely. Users already expect some kind of government sanction against those who harm individuals via cyber means, and borders make historical and cultural sense for denizens of modern states.[23] Finally, a cyber border fits more easily with the institutional compromises and allocations of responsibilities already existing in the governance structures managing modern democracies.

First, the technology of cyberspace is man-made. It is not, as described by the early "cyber prophets" of the 1990s, an entirely new environment which operates outside human control, like tides or gravity.[24] Rather, as its base, the grid is a vast complex system of machines, software code and services, cables, accepted protocols for compatibility, graphical pictures for human eyes, input/output connections, and electrical supports. It operates precisely across narrow electronic bands but with such an amalgamation of redundancies, substitutions, workarounds, and quick go-to fixes that disruptions can be handled relatively well as long as everyone wants the system to work as planned.

However globally interconnected, cyberspace is dependent on preventing its internal need for precision being hijacked or massively disrupted by malicious or hostile actors. States are learning that everything about today's grid can be technologically regulated. There are many points of opportunity for the national government interested in controlling what

eventually ends up being received on Internet desktops, laptops, mobile devices, or even independent appliances in homes and businesses. While connectivity is global—now increasingly found everywhere like land, air, sea, and even space—what is known as cyberspace *is* and *will* remain always man-made, -sustained, and -enabled. And, unlike the sea, land, air, or space, it can be unmade. Furthermore, land expanses, seas, air, and space quadrants do not exist only if information is flowing. Seeing a mountain does not automatically connect one individual to the next or even offer one useful clues about it, yet being on one node does connect individuals to others in this cybered underlayment, even if only with some hacking. Air masses are air masses, but strings of cyber bytes already have information in the way they connect from node to node in protocols. It would be as if a car could not continue on the freeway without broadcasting its VIN number, license, weight, and other data each time it approached an exit. If not approved to continue by the owner of that freeway node, the car would be forced off onto another road.

Today, someone and some firm or agency built or bought now runs and must maintain every single connection on the Internet. Even peer-to-peer (P2P) networks require a person to connect and maintain them. Some firm must develop the software to allow connections, and someone must also code the application allowing the exchanges of data, for good or ill. Today the technological filtering occurs largely through private or semi-private institutional intermediaries. Across the bulk of democratic and nondemocratic states, ISPs are finding their ability to continue to provide services is increasingly dependent on providing filtering services determined by large, state-level authorities. There is no technological reason why these services cannot continue as regulated utilities, nor is there any reason why governments cannot control what runs into the nation from overseas cables or runs out of the nation to criminally harm citizens of other nations.

It is technologically possible for governments to require source tagging of bytes at some point to assure the passage of legally acceptable streams of data or applications or volumes of requests as a way to curtail attacks on their soil or emanating from their soil illegally.[25] Changing the mix by social accord via government action changes the system as we access it, know it, and use it. If key cable junctions are broken, the Internet fails or slows to a crawl for whole nations. If the same cables are merely redirected through an extra set of computers which reject or delete unwanted patterns

of data, then the Internet at the far end of the redirect will seem to be all that it was. Deleted material will simply never show up. With sufficient investment in leading-edge speed cables, inserted filtering servers, and capable transmission lines, it is possible to have a border that is not visibly intrusive to the vast majority of citizens and conceivably even faster than today. For example, while it is widely known China controls its Internet, it is not widely known that this control rests on having only three main Internet gateways between its one-billion-plus population and the rest of the globe.[26] For the kinds of controls exerted by the Chinese government to go unnoticed by users is one piece of evidence that a border for every state, each with different security goals, is within technological reach, if not yet legally and formally sought.

Second, physical borders are known, accepted, and desired by citizens in modern civil societies, and that psychological comfort will be no different for the creation of borders in cyberspace. The relevant emphasis is on "borders," not on universal control of all cybered transactions occurring entirely within the boundaries of a democratic nation. Historically, citizens accepted borders as a security-enhancing necessity against external uncertainties undermining internally accepted rules of interaction. Without such limits, the collective sense of belonging is more easily undermined, as are the rules of civil behavior. Even a willingness to abide by norms of trust and nonthreatening behavior is tied to security, where collective rules can and cannot be enforced. To live in ungoverned societies is not only insecure; it is also a psychologically palpable existential threat. As Joel Brenner explains,

> Constitutive rules define the structure of a given society, as well as the relationships that exist among the individuals that comprise that society; they also allocate essential tasks among the members of the society and ensure that these tasks are performed. Human societies have consisted of bounded systems situated in a delimited spatial area and composed of a defined populace (e.g., "the people of Rome," "the American public," and so on). These spatial and population constraints facilitate the operation of the constitutive rules: spatial and demographic isolation make it easier to socialize those who populate a society so that most accept and abide by its constitutive rules. They also make it easier to identify and suppress those who do not.[27]

Civil society deepens and strengthens when the expectation of modern liberal and universal social rule observance is justified routinely. Historically, the hostile or predatory deviations from actors outside the social jurisdiction of a modern state is exactly what citizens in their implicit social

contract seek to avoid in according a territory their allegiance and legitimacy. Safety at home for the citizen in a highly digital society is a social-psychological need obliging the modern democratic state to act.[28]

Third, borders fit institutionally into the existing architecture of national systems management. Most nations make a distinction between the forces defending the borders from attack (militaries) and those protecting the individual citizens inside the nation from attack (police). This distinction is one of the direct outcomes of the rise of the modern state from the Westphalian Peace. But it is severely challenged by the unfettered character of the current global cyberspace topology. Today militaries, police, and intelligence organizations in particular have been challenged both by the attacks and by the jurisdictional lack of clarity in obligations and ability to demand resources. Both state and nonstate competitors have used the interconnectivity inherent to the web to attack and disrupt operations and gather intelligence about capabilities and intentions across borders with impunity. This is especially true for the United States and other nations highly dependent on telecommunications for command and control; intelligence, surveillance, and reconnaissance; and the management of logistics. Moreover, many military and intelligence organizations have grasped the offensive possibilities of the cybersphere to reach past the borders of other states directly, in concept at least, into the homes of an opposing state's citizens. Across the military communities of the more modern states, information operations and strategic communications programs have been developed to influence adversaries and allies. Physical or "kinetic" attacks are now routinely facilitated by efforts to exploit enemy cyber vulnerabilities.[29]

Without the legitimating and bureaucratic clarity of a virtual border, for example, jurisdictional disputes in nations observing centuries of criminal versus national security civil society laws are hamstrung to respond. Stuxnet easily crossed borders as intended by its designers. If it were a nonstate actor, then the action is criminal, invoking the powers of police forces. If it were a state-level actor, then militaries would be involved. Today it is not clear which groups were involved, in large part because the electronic trail of possible attribution moves readily across states, and states have no obligation to sanction bad behavior emanating outward from their territory. Nonetheless, a state's facilities were harmed, and many states are viewing that uncertainty and inability to lay blame and attribute the attack as unacceptable vulnerabilities.[30]

In principle, only from ungoverned or ungovernable territories do modern groups launch destructive missiles on neighboring nations without automatic interstate calls for sanctions. With physical borders, states that wish to be accepted internationally are obliged by law and custom to stop the attacking behavior of their residents or to allow the offended state to reach inside to stop it. Once the virtual limits of sovereign power can be demarcated in the global cybersphere, states ignoring or supporting massive denial-of-service attacks from their territories will be held internationally responsible. Domestic legal systems that today do not have internal laws criminalizing predatory cyber behavior affecting other states will have to initiate the kinds of internal controls already presumed in international policing. If they do not or if they actively promote the external attacks from their territory, just as in centuries of physical conflict, they will have to acknowledge the right of the attacked states to defend across borders if necessary. Distinguishing criminal laws and activity from national security missions and jurisdiction becomes enormously more manageable when the jurisdictional lines are drawn and recognized in a new cyber-Westphalian process.

Managing the bordered virtual sphere will also enable a third swathe of cyberspace to be identified as well—the ungoverned badlands equivalent to the very physical regions of failed or failing states. As civil society extends into cyberspace with rules of accepted behavior and reinforced by modern state institutions, it becomes easier to invoke the routine activities of international organizations to curb, if not cure, the disruptive activities of the failed-state portions of the international virtual globe. As a result, institutions will adapt and adjust while replicating the functional aspects of the current physical concords and rules of behavior to contain the harm by actors who deviate from the emerging virtual civil world. What is happening today in the slow civilizing of cyberspace, however scattered and seemingly unique, strongly depends on what individual governments see as either the threat or the leverage they have and the institutions they develop to act on those perceptions. For all, the beginnings of a need to control the sovereign, albeit digital, national territory is already present. None are controlling the harm, transmission, laws, or sanctions emerging on the sovereign territory of another state; rather, each is operating under the modern notion of monopoly of power on the territory already demarcated and looking to its own laws and control of actions on its territory, to include network connections.

Emergent Virtual Borders

Indications of emergent borders within the cybersphere are appearing at many levels, making for a variety of models across the current extent of sovereignty the state presumes or seeks. So far some are quite singular. China leads the authoritarian states in a more ubiquitous cyberspace regulation model aimed at controlling information from outside and circulating inside its borders. In this "all points" model, the border boils down to gateways largely filtering information with the ability, in principle, to curtail the Internet connections, either between internal regions or between China and the rest of the world. It is a technological (limited gateways), institutional (regulated telecoms), and psychological (cyber self-censors and vigilantes) model operating on many levels at once.

In this model, China is expressing a long-standing concern for the stability and security of the well-established Chinese territory. "Whether we can cope with the Internet is a matter that affects the development of socialist culture, the security of information, and the stability of the state," President Hu of China said in 2007.[31] In the 1990s, the Chinese Communist Party recognized the power of unfettered access from/to Chinese citizens and declared the Internet to be a fifth area of territoriality to be nationally secured. They built the "Golden Shield" that employs an estimated 40,000 Internet police who in 2009 shut down about 7,000 websites, deleted 1.25 million pieces of information, and arrested 3,500 people, including 70 dissidents and bloggers now in jail. In addition to directly controlling the content, about 30,000 netizens are employed part-time to intervene in online forum discussions and redirect conversations away from sensitive topics. The Chinese leadership routinely characterizes Westernized social media as subversive tools and sees the hand of the United States in diplomatic subversion in any US–sponsored discussions of open Internet. With the view that state security and social stability are under attack, the Chinese government implemented the strong, technologically sophisticated, heavily intelligence collection–driven second phase of the Golden Shield in 2010.[32]

For at least six years, China has also been working on constructing its own Internet. In what is called China's Next Generation Internet (CNGI), the current limited number of Internet addresses expands massively by adding enough digits (IPv6)[33] to provide every single machine connecting to the Internet its own unique web address. This addressing protocol also means every single web transaction can be tracked from the original machine

to any other, allowing a massive societal control advantage when linked to other rapidly emerging advances in the raw computing speed and storage of computer systems. Not only will three-dimensional online worlds move faster and more realistically, but also every interaction in those worlds can be recorded or individually tracked in real time to the specific machine.[34]

A new, more surveillance-friendly addressing system is useful to the Chinese or any government desiring to control its own borders without having to use proxies or agents to do their controlling. The so-called Great Firewall that Google declined to support in 2010 was in reality the imposition of liability onto ISPs if one of their users accessed forbidden sites or topics.[35] As Google demonstrated, this "intermediary liability" approach to control has its limitations for a nation known to have a cultural preference to avoid proxies.[36]

The justification of these measures as essential for citizen safety against social disharmony, false information, fraud, piracy, and social ills such as pornography is a common theme in the oft-times bumpy path to creating a sovereign border in cyberspace. For example, in 2005 the Chinese announced an upgrade to the national text messaging filtering system with automatic police alerts when false information, reactionary remarks, or harmful activities such as fraud and scams are found in cell phone texts. In December 2005 the vice-minister of the Ministry of Public Safety announced that the upgraded system's 2,800 surveillance centers had tracked about 107,000 illegal cell phone text messages in November 2005. With about 33 percent of the texts associated with criminal fraud activities, 9,700 cell phone accounts were shut down over the month.[37] At the time (2004), Chinese citizens annually sent 218 billion text messages, against which an objectionable number of 107,000 is not even a drop in the bucket. By 2010, however, the addition of supercomputers which can move trilobits per second provided advanced capabilities to filter cell phone text messages centrally. The police, using undisclosed criteria, create lists that cell phone companies must use to scan all customer text messages. Companies must automatically suspend the accounts and report the incidents to police if banned terms are found.

The new technologies have enabled not only massive increases in the intrusive and comprehensive search mechanisms but also more punitive measures against those found to violate the restrictions. During the same period of slowly gaining control of all communications media, the Chinese authorities have closed websites, especially those able to share files, and

increased the difficulty for citizens to have their own sites.[38] Already the Chinese government has channelled the physical access of all web traffic in or out of China through three major gateways in Beijing, Shanghai, and Guangzhou.[39] Whether or not the international community approves, China's government is engaged in using the accretion of internal controls on content as a consistent part of a state asserting sovereignty over key aspects of its internal social territory.

Several democratic nations have charted a "key firm" model of regulating the large telecoms, albeit loosely, with the goal of curbing malicious or thieving activity, not information flows. These include Australia and to some extent Germany. Major Westernized, largely European democracies are enacting or strongly considering enacting Internet control measures to prevent theft or abuse of their citizens' personal information and the economic assets of their countries. Others, such as the UK, turned initially to pan-agency coordinating economic or social, but not security, institutions to encourage, monitor, and guide internal Internet transactions. The goal is to curb foreign and local theft of national economic assets and private personal information. More recently, however, even European nations have shown an increasing tendency to see a role for national security controls, although less prominently discussed. In 2008, Sweden passed legislation allowing its national police force's intelligence section to monitor all Internet traffic in and out of the country, whether by Swedish citizens or others. It was challenged widely and loudly by prominent privacy advocates, but the law withstood challenges as a central piece of anti-terror legislation and was institutionally implemented in late 2009.[40] The model is still firm based but is increasingly more focused directly on security.

The path to a national border in cyberspace may not prove as difficult for EU nations as it would for other sectors because cyberspace policies are currently left largely to member states. The level of security varies greatly across nations, and it is unlikely the UK will, any more than France, wait for an EU–wide solution to threats to its own cyber resources or citizens.[41] The UK, in particular, has moved incrementally to lay the foundation for a national border, sometimes for political reasons having little to do with cyberspace, such as a national identity card to curb illegal immigration. The rise of serious intrusions into sensitive government networks—at least 300 over the course of 2009—has pushed the island state to construct two agencies with the specific missions of coordinating and informing the tools, tactics, and targets of cyber security across all governmental

agencies.[42] Current trends suggest the UK will be closely behind the United States over time as the elements of a national border in cyberspace are erected, in large part because the UK, as a close partner of the United States, is both more of a target and more informed about its vulnerabilities than other EU nations.

The singular marker of an emerging border, however, is the creation of a military organization—a cyber command—to protect the nation from the kinds of harm that historically only a peer state or neighbor could inflict. For a nation to establish such a unit and publicly declare to have done so, that state is explicitly saying it has territory to defend and the threat to be met poses conceivably an existential threat. Such a unit marks the acknowledgement of a nationally owned space that the nation values and will protect using available and appropriate resources, including regulatory, law enforcement, and military capabilities. That the borders have not yet been recognized by other nations—a key outcome of the long Westphalian process—does not diminish the significance of this institutional declaration of sovereignty to be defended, by definition, in cyberspace itself. While not as advanced as either China or Australia in controlling their domestic Internet access or policing its key industries, the United States in establishing its new US Cyber Command has laid the cornerstone necessary for a national cyber border. The nation has stated an intention to defend against, repel, or prevent whatever could come across its cyber border and do so with its military might and resources if required. The declaratory aspect of this unit is important as a permanent symbol of a new cyber–Westphalian international system. China has government organizations with what Western observers presume are the same missions as Western cyber commands, but they are not publicly named as military defenders of the nation. The "cyber command" model primarily rests on the use of national security institutions for cyber defense at and beyond a border.

Cyber Command—The US Model

In the fall of 2010, the US Cyber Command became operational after an exceptionally rapid year of institutional and legal preparation.[43] This institutional response to the rise of the cybered conflict age emerged to anchor a future cybered border for the whole nation. Its initial mission was to protect only military organizations from cyber attack, but as soon

as a military unit existed to create a cyber safety wrapper around US critical military assets, political statements emerged about creating the same protection for the whole nation.[44]

From the RMA to net-centric warfare, the United States has a history of providing new models for national-level security organizations, especially military organizations.[45] For the United States to announce a new national cyber command automatically provokes a new debate in the international military and legal communities.[46] Whether or not other nations need, want, or can afford to have a singular military unit focused on cybered conflict, their leaders, doctrine writers, and strategic thinkers will contemplate whether they themselves need such a unit when the remaining superpower signals how critical it is for national security.

If patterns of military emulation occurring since World War II hold true, the vast majority of nations will inevitably have something that looks and acts like a national cyber command, whether or not it initially bears that name. Already we have seen nations closely associated with the United States either mirroring it in creating their own cyber command or declaring an interest in having a unit that approximates the functions of US Cyber Command. South Korea, for example, now has a military cyber command after enduring a massive assault in early July 2009.[47] In recent strategy discussions, the United Kingdom, while focused on the cyber protection of the entire society, has begun discussing closer integration of its military cyber resources with its intelligence cyber resources and the challenge of knowing when to use offense versus defense when a threat emerges.[48]

Importantly for the emergence of borders in cyberspace, the US model of a national cyber command has several distinctive elements. First, the unit chosen by national leaders as their initial foray into strategic national security in cyberspace was a military, not a civilianized, internal security agency built for disasters or crime. With the weight of US resources to dedicate to a strategy of purely defensive mitigation from cascading surprise attacks, policymakers chose a natural experiment that clearly reinforced the idea that simply waiting for the attacks to hit and then mitigating the effects inside the physical borders is likely to be devastatingly insufficient. Militaries operate at the edges of nations in the modern state or deployed forward to prevent attacks. Choosing a military to be primus inter pares in cyber security also reinforces the seriousness of the existential threat, as these institutions are historically the last resort of national

survival. Creating US Cyber Command has redirected much of the global conversation about cyber security from merely blunting attacks after they arrive to repelling or disrupting the attacks before they cumulate into great harm. If cyber security is a mission involving military-like actions repelling attackers, then borders will have to be determined to guide when and where these actions can occur.[49]

Second, while the mission of the US Cyber Command is currently to protect US military cybered interactions, the structure of the new command is clearly intended to blend operations to benefit simultaneously from what was traditionally considered offensive and defensive cybered operations and the collection of global intelligence. In cybered conflict, the offensive advantages of the attacker lie in relatively easily attained preemptive surprise using the intrinsic difficulty of predicting cascades in globally large-scale complex systems. The result is that a good defense requires the ability to successfully operate offensively, knowledgeably, and rapidly to preempt the preemptive attack, or at least anticipate it with sufficient time to prepare and mitigate its effects. The peace versus war distinction has very little meaning operationally in the current frontier-like nature of global cyberspace, and the US Cyber Command model directly acknowledges the loss of this strategically and internationally accepted distinction by dual-hatting its commander as the head of the premier electronic intelligence agency, the NSA, and the military commander of the new cyber command.[50] In that Hobbesian choice, the blend of intelligence and a decision to act offensively occurs in the internal deliberations of one man subject to national laws but able to act quickly and knowledgeably if necessary.[51]

That the cyber command has the ability to attack, defend, and collect information globally is an innovation critically important not only for the United States but also for the wider international community resolutely tied to seeing conflict and peace as distinct. While the concept of a Cold War or an international crisis is routinely understood and used in characterizing disagreements, war is distinguished from peace to clearly politically and psychologically guide international institutional actions, negotiations, and strategic expectations. Unfortunately, cyberspace by its dual-use nature and ubiquity can be simultaneously hot, cold, warm, or turbulent in different parts of the world. The US innovation made it clear the last superpower thinks security rests on acknowledging that emerging reality with a unit commanding serious attention by would-be attackers.

Put differently, the model demonstrates a conclusion—that offense, defense, and extensive knowledge collection are needed to be secure—and a hypothesis that the best way forward is to build on the already organized structures of a military. For the vast majority of European democracies which have a great deal of difficulty in publicly and politically endorsing offensive measures in cyberspace, cyber security institutional adaptations have been incremental, mired in lengthy debates on civil liberties and economic progress threats. The exceptionally rapid implementation of the cyber command model by the United States has broken the allies' collective cognitive logjam. Now, whether or not senior leaders agree in principal with the solution, they are discussing new organizations and responses for repelling a threat capable of existential damage; not just burglary or theft, but massive undermining of the economic health of the state. The developments of the Confiker worm, widening ravages of international cyber crime, and lastly the unsettling discovery of Stuxnet and its success in a critical infrastructure have sparked a strong new interest in the US model, at least as an alternative.

Becoming more widely accepted is a growing national need to consolidate the efforts of the state for protection against an extraordinarily complex set of possible hidden, lightening fast, and massive threat avenues. It occurred to every successful medieval leader that one needs moats, walls, watch towers, and guards, but also one must have rapid-reaction horse- and/or ship-mounted units to keep the worst attackers far from the capital. A national unit blending all those age-old functions in cyberspace becomes a logical consideration.[52] Within a year of constructing two distinct units for cyber security—one at the Cabinet level—the change of British government in 2010 resulted in a stronger link between these units and budget increases for cyber. Furthermore, the new government declared cyber threats to be a top-tier national security issue.[53]

Similarly, in late 2008, France published the first defense white paper since 1994 and not only added the concept of whole-nation security but also elevated cyber security to one of four key national threats. The mission was to create an institution capable of guiding the other agencies in protecting the entire nation's national cyberspace. In the process a small, formerly secretive organization has become its central and publicly discussed Agency for National Information Security (ANSSI). Over the course of its first year of existence, 2009–10, the organization has helped research and justify legislation to allow further central control of defensive

and, if necessary, offensive national cyber means.[54] Other nations, especially those with limited cyber resources such as the Baltic States, are notably pushing strongly for NATO as a military organization to be designated as guarantor of their national cyber security, especially if cybered means accompany physical assaults to undermine the nation's resilience.[55]

Third, by making US Cyber Command across rather than separate from the four military services, the new organization carries within it the seeds of its future elevation in importance for the nation. As concepts for repelling attacks aimed beyond military forces at the heart of the United States have begun to coalesce politically, critical practical decisions will be made about where the tripwires are to be virtually drawn and maintained. The model does not make a small unit that simply supports other government actors in the military. Rather, its size, prominence, and position atop subordinate service-only cyber commands reinforce the universality and possibly existential importance of the task to the whole nation beyond the .mil community. All the services are involved, and all of them are required to contribute to a coordinated national response to a major event involving US military elements. Only a few threats—such as nuclear war and terrorism—have forced such rapid, unequivocally collective and ubiquitous responses beyond traditional physical domains of land, air, sea, and space.

Recently, a memorandum of agreement between the US Department of Defense and the Department of Homeland Security (the lead agency for national cyber defense for government agencies and critical infrastructure) formally initiated a process for the DoD to aid the DHS in the event of cyber-related catastrophes. The memorandum clearly invoked the direction of the support from the cyber-saavy DoD (read NSA and US Cyber Command) to the cyber-responsible but overwhelmed DHS.[56] In this, another step is taken toward a national notion of a cyber territory to be defended, a virtual space involving the whole of the society. The terms of crossing over from border and outward duties for the military to inward, more-domestic missions as a function of an anticipated cas extremis underscores both the importance and the need to have identified the border itself to regulate these agreements.

Fourth, the offensive operations mission of any cyber command working for a democracy underscores the need for other democracies to establish their own borders in cyberspace to demand noninterference in practice as well as de jure. The US Cyber Command model leaves unanswered the question of bad actors operating from within one democracy operat-

ing outward to harm other democracies. This lack of clarification of the precise operational rules of engagement and reach was left unresolved in part because the debate on that legal authority alone could have stalled the creation of the cyber command and the defense it provides.

Leaving the debate open to discussion with allies and other democracies allows for parsing out the actions of allies, especially in NATO. Experience will channel the next range of evolutionary steps for all concerned, but there is an unspoken presumption, especially among senior NATO partners, that Western democracies in particular are united in wanting security in everyone's cybered systems. Nonetheless, while the United States is unlikely to see its new cyber command as threatening allies, that benign assessment is not universally shared. Many parties on the left in many European states are routinely concerned, with good historical reasons, about the concentration of power in government hands. For example, Germany is creating a centralized cyber-crime facility that would support de facto if not de jure an emerging all-source cyber-crime service. The facility will be built, but the unified analysis seen as key will not occur among permanent cadre due to Green Party politicians' fears of concentrated data on citizen actions being in the hands of the federal government. As a result, the facility will be more of a repository that individual agencies may consult as needed. The deliberate dispersal of organizational interaction defeats the concept intrinsic to an organization such as US Cyber Command or, for that matter, a centralized cyber security operations center (CSOC) as set up in the UK.[57] This fear, however historically justified and currently endorsed, is more likely to view the US development of a virtual border with skepticism and some concern with the extent that a military cyber command is attached. In particular, they are likely to be more interested in a border in cyberspace for their own nation to have the ability, if necessary, to constrain US government actions in cybered preemption that are anticipated to harm European citizens.[58]

At the end of the day, both friends and enemies will be further incentivized to consider their own ability to demarcate in boundaries and defend in institutions their own national slice of cyberspace.[59] Creating US Cyber Command is only one mark of transformation, but it further accelerates the state-level interest in acquiring greater control of the uncertainties of the rapidly declining cyberspace frontier. This transformation is not only natural for the new cybered conflict age, it may be desirable for a future

civil global society still interconnected but with international rules guiding interactions.

Resuscitation of International Relations Theory and History

With the establishment of borders in cyberspace, everything we know about deterrence, wars, conflict, international norms, and security will make sense again as practical and historical guides to state actions and deliberations. With a border in and enforced by technological means, also essential will be the means to monitor who is electronically crossing the line in the virtual sand and whether that passage of bytes is permitted by national law, either criminal, civil, or national security. These means will have to be maintained and adapted to emerging new threats. These mechanisms will be a combination of encryption, unique machine/user identifiers centrally controlled, and local hardware-human "bio"-metrics. No more would the near-Herculean task of tracking bad cyber actors on a massive scale hinder a normal civil society's desire for a functioning mechanism to deter that source of harm. A border in cyberspace necessarily presumes some form of verifiable and current originating data for everything trying to pass into the nation, from bytes to malware to phishing or mass assaults. The nature of connectivity and emergence of other states means bad data which comes from someplace will necessarily come from some territory of some state with overarching responsibility for allowing such transmissions to continue. No longer can a state claim it is not harboring those attacking every .mil address in the United States while encouraging their internal development of "patriotic" hacking skills and a blind eye to those who hack outwardly only.[60]

In the bordered future world of digitized states, actual hot war will also be forced into expressions that can be recognized. Cross-border attacks will be regarded as such, even if largely cybered in their characteristics. If the sponsoring state refuses to stop the attacks or to allow the defending state to reach inside its territory to stop them, then the sponsoring state can be presumed to support them. Conditions much like the onset of war can then be said to exist. Wars albeit cybered will have all the pieces we have seen over the course of centuries, to include tensions, collateral damage, revenge myths, and arms races. We will deal with war as well as its

phases in warmth, cooling, and even termination en route to civil or at least calm relations as well as we were likely to do without the Internet.

It is not clear what alternatives exist in any case. It is far from clear that global civil society was enhanced in the world's poor or floundering regions by freewheeling access to every human pathology allowed by the two decades of the Internet. Those who benefited from the looseness already had a civil society in their national democracies and standards of decent behavior plus social norms on predatory behavior. Nor was the civil society goal of fairness and stable international development advanced by the wholesale secret extraction of technological advantage by one large mercantilist nation in particular pilfering massively and widely the industrial hard drives of other more-advanced nations. Those states whose firms and societies paid for the research and development have lost competitive advantage across their economies not only in jobs but also in basic resources on which to build future technological advantages. The communities of love and toleration envisioned by Rheingold in the 1990s did not flower save in small middle/upper–class educated communities; even social networking sites quickly developed predators, cyber bullys, and stalking. Today, even the original uptopian social chat site, "the Well," refuses anonymity.[61] It seems communities of hate, exploitation, and fraud grow as fast, if not faster, than the open, sharing, and enhancing virtual societies.[62]

With the rise of a national interest in protecting their own cyber turf, international norms will be negotiated state by state, region by region, coalition by coalition, and international regime by international regime. Cyberspace is man-made, and its commons-like characteristics can be negotiated across borders just like food production and safety, trade subsidies and streams, banking reserves and credibility, and even whaling. Life on, around, and through the virtual borders will be as turbulent, semistable, and prone to smugglers, free riders, would-be upstarts, and annoyances as the physical borders are now in harbors, airports, land crossings, and maritime lines of control. According to British prime minister Gordon Brown in 2009, "Just as in the 19th century we had to secure the seas for our national safety and prosperity, and in the 20th century we had to secure the air, in the 21st century we also have to secure our position in cyberspace in order to give people and businesses the confidence they need to operate safely there."[63]

Many unique concerns of key nations will continue as well, perhaps easier to pursue when national cyber borders are consensed upon. For

example, one would expect no change in Germany's demand for national cultural reasons to close its ports to neo-Nazis and chase smuggled peer-to-peer Internet sites that encourage attacks on brown-skinned people, just as Saudi Arabia will close off pictures of women in positions of power and chase P2P porn sites and dissidents internally. The Chinese bureaucracy will refuse to agree to international constraints on its national right to execute addicted online game fanatics who commit crimes and jail those who smuggled pictures of the Dalai Lama or a real CNN headline internally. Tunisia and Libya will simply not talk about their internal controls and demand the usual physical rights to do technologically what they will. Status quo pro ante will adapt to the emerging topology across the globally connected socio-technical world.

Today, the United States has declared cyber threats to be at the top ranks of national security concerns, created a new major military unit, and moved along a multitude of fronts to shore up its own national ability to forestall destructive cybered cascades operating from cybered means. But normalcy also requires recognition of the international community's role in reducing interstate cybered threat just as borders may rise to protect a particular state. If attackers are limited by borders in the number of states they can attack at once using cybered means in their operations, they are forced to forage for weaker national structures or concentrate their resources on their main objectives. More states will be unaffected by mass attacks and will be able to develop essential internal and collective regional resilience to the surprise attack that the sheer complexity of cyberspace inevitably allows.[64] The more unaffected states there are who are also allies, the more likely these unaffected states will have the resources to offer mutual support to defending states.

Finally, the United Nations as an international forum negotiates between states whose roles, responsibilities, and territories are established. Its agencies and commissions will provide mechanisms for nations to quietly and practically cooperate even if they publicly are at odds. When cyberspace becomes a more normalized international system for modern states, one might see cyber ambassadors at UN agencies or cyber attachés at embassies to physically and rapidly calm crises or to coordinate responses if cyber systems are under assault.[65] Rules of conflict resolution and acceptable cybered civil society engagement are collectively, not individually, developed and enforced. When states are cybered entities with sovereign boundaries and can represent and defend themselves in the face of cybered conflicts, a relatively

less predatory and chaotic era of cybered states and rule regimes is likely as the globe continues its relentless digitization across all facets of human society.

Conclusion

In the near future, states will delineate the formerly ungoverned or chaotic cybersphere by formal agreement. In the new cyber–Westphalian process, digital regions complete with borders, boundaries, and frontiers that are accepted by all states will inevitably emerge. The rising virtual mirroring of what has been painfully carved out in the concrete world is not all that undesirable for societal stability, economic returns, and international security. Individuals, a wide variety of social organizations, and, certainly, most forms of commerce thrive on order and regularity. In the material world, we know how to handle cross-border wars and attacks in ways that we struggle nearly in vain to handle cross-border embedded, grey threats masked by the density of modern processes. In the cybersphere, borders will emerge internally within nations as well as externally as the usual commercial and personal security bulwarks against free riders and thieves. Once the borders have emerged, police and national laws will hold sway as they do today in the modern nation-state. However, in much the same way as they operate today in the physical world, attacks across borders will become state responsibilities, whether or not the state approves or guides the attacks.

As the process emerges from inklings to the self-evident, the implications of pulling cyberspace back into the known world of international relations are profound. Today a rough consensus is emerging that something about the frontier nature of the web has to be regulated, either by individual states or by enforceable international regimes. But until the last few years and the dramatic success of the Stuxnet attack, the debate was as much about an international regime as it was about a nation-by-nation response. The international regime approach, however, is fraught with time and attribution difficulties. Not only can such a regime take decades to build, enforcing it as the web stands today will require the very thing current topology of the web does not offer—a way to verify the identity of (and therefore sanction) the violator. The result is, wittingly or unwittingly, individual states have started down the path on their own toward controlling the way the web affects their citizens, organizations, and critical elements of the society. The transition, of course, still lies ahead. SSQ

Notes

1. *Cybered conflict* differs from *cyber war* or *cyber battle*. The latter is fully technological and could, in principle, be conducted entirely within a network. It is normally a component of the former. A cybered conflict is any conflict of national significance in which key events determining the path to the generally accepted outcome of the conflict could not have proceeded unless cyber means were nonsubstitutable and critically involved. The terms are distinctively and deliberately used in this article.

2. Nicolas Falliere, Liam O. Murchu, and Eric Chien, 2010. "W32.Stuxnet Dossier: version 1.3," http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

3. Susan W. Brenner, "Distributed Security: Moving Away from Reactive Law Enforcement," *International Journal of Communications Law & Policy* 9 (December 2004).

4. For example, as the critical infrastructure of Westernized nations such as the United States is moving online for automated 24/7 services with less labor or greater precision, the loss of a central server for the infrastructure of even small communities could prove devastating. In early 2010, a thief stole the one single computer running the automated system providing clean water for the town of Molalla, OR. Had the thief wanted to harm the citizens, taking over the computer remotely to disrupt or destroy the water filtration system would have been exceptionally easy. Even the apparently mistaken theft could have been worse had the thief simply used the machine in situ to ruin the filtration system or poison it. "Theft In Molalla [Oregon] Reported To Department Of Homeland Security: Computer Controlled Town's Water System," *KPTV.com Homepage: Portland News*, 26 March 2010.

5. Isaac Porche, "Stuxnet is the world's problem," *Bulletin of the Atomic Scientists*, 9 December 2010.

6. David E. Sanger, "Iran Fights Strong Virus Attacking Computers," *New York Times*, 25 September 2010.

7. J. B. Michael et al., "Integrating Legal and Policy Factors in Cyberpreparedness," *Computer* 43, no. 4 (2010): 90–92.

8. Threats are considered so serious that cyber-security officials are now expected to have training in known hacker methods. Bill Gertz, "Inside the Ring: Hacker Training," *Washington Post*, 4 March 2010.

9. Nigel Kendall, "Global cyber attacks on the rise: 75 percent of companies have suffered a cyber attack, at an average cost of $2 million, says Symantec security survey," *Times* (London), 22 February 2010.

10. Gillian Wong, "Chinese police shut down hacker training business," *Washington Post*, 8 February 2010.

11. The history of the American railroad, for example, included reaching out to the towns along its path to control the uncertainties that independent but gouging store owners imposed on the passing freight lines and passengers. Renate Mayntz, "The Changing Governance of Large Technical Infrastructure Systems (LTS)," in *Conference Paper: Complexity and Large Technical Systems*, Meersburg, Germany, 2008.

12. Given human history, it does not much matter what precisely initiates the conflict; rather, it is the dependence of one or both parties on a pass, waterway, or global underlying socio-technical system that determines the targeting on those items. Nomads had no fixed address, but they certainly had a sense of their rights to seasonal food crops and were willing to fight to exclude other groups to assure their own survival. R. L. O'Connell, *Of Arms and Men: A History of War, Weapons, and Aggression* (London: Oxford University Press, 1989). See also Charles Tilly, *Coercion, Capital, and European States, AD 990–1992* (Malden, MA: Blackwell Publishers, 1992).

13. Stephen Krasner, "Shared Sovereignity: New Institutions for Collapsed and Failing Status," *International Security* 29, no. 2 (Fall 2004): 85–120.

14. Charles Tilly, "Cities and States in Europe, 1000–1800," *Theory and Society* 18, no. 5 (1989): 563–84.

15. Rajesh Tandon and Ranjita Mohanty, "Civil Society and Governance: A Research Study in India," in *Global Comparative Research Study on Civil Society and Governance* (Sussex, UK: Society for Participatory Research in Asia, 2000).

16. Joseph S. Nye Jr., "Cyber Power," Harvard Kennedy School, 2010, http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf.

17. Duncan B. Douglass, "An examination of the fraud liability shift in consumer card-based payment systems," *Economic Perspectives* 33, no. 1 (1st qtr., 2009): 43–49.

18. Ross Anderson et al., "Security Economics and European Policy," in *Managing Information Risk and the Economics of Security*, ed. Eric Johnson (New York: Springer, 2009), 55–80, http://weis2008.econinfosec.org/papers/MooreSecurity.pdf.

19. D. Lindsay, "Liability of ISPs for end-user copyright infringements," *Telecommunications Journal of Australia* 60, no. 2 (2010).

20. Michael Evans and Giles Whittell, "Cyberwar declared as China hunts for the West's intelligence secrets," *Times* (London), 8 March 2010.

21. Elinor Mills, "Web traffic redirected to China in mystery mix-up," *CNET*, 25 March 2010.

22. This effect, according to John Mallery, is a national cyber security means of increasing the "work factor" of the bad actor. The key strategic goal of cyber defense is to raise the work factors for attackers and to lower them for defenders. Work factors are conceptualized along dimensions of computational complexity, cost, cognitive difficulty, risk and uncertainty, cultural factors, and information differentials. See John C. Mallery, "Towards a Strategy for Cyber Defense," presentation at the US Naval War College, Newport, RI, 17 September 2010.

23. Douglas M. Gibler, "Bordering On Peace: Democracy, Territorial Issues, and Conflict," *International Studies Quarterly* 51, no. 3 (September 2007): 509–32.

24. Narushige Shiode, "Toward the Construction of Cyber Cities with the Application of Unique Characteristics of Cyberspace," *Online Planning Journal*, 1997, http://www.casa.ucl.ac.uk/planning/articles21/urban.htm.

25. On this point of curbing outward attacks, a functioning government controls the means of violence within its nation and that would include the means of enabling one of its citizens to attack another nation without governmental approval.

26. Kathrin Hille, "How China polices the Internet," *Financial Times* online, 17 July 2009.

27. Joel F. Brenner, "Why Isn't Cyberspace More Secure?" *Communications of the ACM* 53, no. 11 (November 2010): 2.

28. Paul Cornish, Rex Hughes, and David Livingstone, *Cyberspace and the National Security of the United Kingdom* (London, UK: Chatham House, 2009).

29. Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Washington: RAND, 2009).

30. Pam Benson, "Computer virus Stuxnet a 'game changer,' DHS official tells Senate," *CNN*, 17 November 2010.

31. Michael Wines, Sharon LaFraniere, and Jonathan Ansfield, "China's Censors Tackle and Trip Over the Internet," *New York Times*, 8 April 2010.

32. Ching Cheong, "Fighting the Digital War with the Great Firewall (op-ed), *Straits Times*, 5 April 2010.

33. Three of the world's largest sites are banding together with two of the largest content distribution networks, Akamai and Limelight, coordinated by the Internet Society, to declare 8 June 2011 World IPv6 (Internet Protocol version 6) Day. "Google, Facebook and Yahoo Partner

for World IPv6 Day," *Softpedia.com*, 12 January 2011, http://news.softpedia.com/news/Google-Facebook-and-Yahoo-Partner-for-World-IPv6-Day-177852.shtml.

34. Ben Worthen, "Internet Strategy: China's Next Generation Internet," *CIO.com*, 15 July 2006, http://www.cio.com/article/22985/Internet_Strategy_China_s_Next_Generation_Internet_ .

35. Rebecca MacKinnon, "Commentary: Are China's demands for Internet 'self-discipline' spreading to the West?" *McClatchy Report: Washington Bureau*, 18 January 2010, http://www.mcclatchydc.com/2010/01/18/82469/commentary-are-chinas-demands.html.

36. Mike Masnick, "The Similarity Between ACTA and Chinese Internet Censorship," *TechDirt* online, 20 January 2010, http://www.techdirt.com/articles/20100120/0216537828.shtml.

37. "China keeping closer eye on phone text messages," *New York Times* Technology Section, 6 December 2005.

38. Sharon LaFraniere, "China to Scan Text Messages to Spot 'Unhealthy Content'," *New York Times*, 20 January 2010.

39. Wines et al., "China's Censors Tackle and Trip Over the Internet."

40. Lucian Constantin, "Attack Hits Swedish Signals Intelligence Agency's Website," *Softpedia News*, 6 November 2009.

41. Evans and Whittell, "Cyberwar declared as China hunts for the West's intelligence secrets."

42. Anthony Lloyd, "Britain applies military thinking to the growing spectre of cyberwar," *Times* (London), 8 March 2010.

43. Lance Whitney, "U.S. Cyber Command prepped to launch," *CNET News—Security*, 23 March 2010.

44. William J. Lynn, "Defending A New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* 89, no. 5 (September/October 2010).

45. Emily Goldman and Leslie Eliason, *The Diffusion of Military Technology and Ideas* (Stanford, CA: Stanford University Press, 2003).

46. Scott J. Shackelford, "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law," *Berkeley Journal of International Law* 25, no. 3 (May/June 2009).

47. "South Korea to set up cyber command against North Korea—two years earlier than planned," *Channel News Asia* online, 9 July 2009.

48. Richard J. Aldrich, *GCHQ: The Uncensored Story of Britain's Most Secret Intelligence Agency* (London: HarperCollins, 2010).

49. Ellen Nakashima, "Pentagon's Cyber Command seeks authority to expand its battlefield," *Washington Post*, 6 November 2010.

50. US laws enable "authorities" to draw legislative lines between offense (a military "Title 10" authority), defense (of military, "Title 18"; or of the wider government, a DHS mission), and the collection of national intelligence (a "Title 50" mission given the National Security Agency as primus inter pares electronic collector among other intelligence agencies).

51. This structural compromise was unusual for the United States, and it was hotly debated in the Congress before the first commander, Gen Keith B. Alexander, was confirmed as head of both agencies. Winning the debate were the need for a very wide intelligence view, a high level of skills, and the military ability to move quickly, as well as the character and expertise of the new commander himself. Ellen Nakashima, "Gen. Keith Alexander confirmed to head cyber-command," *Washington Post* online, 11 May 2010.

52. Even the loss of laptops, treated casually just years before, now engenders enormous legislative concern and recriminations against agencies even indirectly responsible for the cyber security of the nation as a whole, such as the GCHQ intelligence agency. " 'Cavalier' GCHQ online spy centre loses 35 laptops—Centre also struggling to keep up with national cyber threats," *Computerworld UK* online, 12 March 2010.

53. Richard Norton-Taylor, "The UK is under threat of cyber attack," *Guardian* online, 18 October 2010.

54. See the website http://www.ssi.gouv.fr/site_rubrique97.html, hosted by ANSSI, which rather openly discusses its successes in strengthening cyber defenses.

55. "EU and US join NATO cyber security pact," *Computerworld UK* online, 10 November 2010.

56. Cheryl Pellerin, "DOD, DHS Join Forces to Promote Cybersecurity." *American Forces Press Service*, 13 October 2010.

57. Private conversation with senior civilian cyber-security police official in Germany, October 2010.

58. Even the Chinese government has felt the need to have a cyber command equivalent and publicly announced its creation of a cyber warfare unit as a defensive measure in response to the provocative actions of the US government in creating a cyber command. Tania Branigan, "Chinese army to target cyber war threat," *Guardian* online, 22 July 2010.

59. "European Union Considers Stronger Cybersecurity, Stricter Penalties for Hackers," *New New Internet* (*TNNI*) online, 1 October 2010.

60. John Markoff, David E. Sanger, and Thom Shanker, "Cyberwar: In Digital Combat, U.S. Finds No Easy Deterrent," *New York Times*, 26 January 2010.

61. Howard Rheingold, *Virtual Communities: Homesteading on the Electronic Frontier* (Reading, MA: Addison Wesley, 1993).

62. Gene I. Rochlin, *Trapped in the Net: The Unanticipated Consequences of Computerization* (Princeton: Princeton University Press, 1997).

63. Tom Espiner, "UK launches dedicated cybersecurity agency," *ZDNet UK* online, 25 June 2009.

64. The process of moving to better internal resilience is elaborated in a forthcoming book. The work argues for and outlines a security resilience strategy involving both disruption and resilience via cybered institutional capacities developed and adapted at the national level. Chris C. Demchak, *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security* (Athens: University of Georgia Press, 2011).

65. Jaikumar Vijayan, "After Google-China dust-up, cyberwar emerges as a threat: The episode highlighted cyberthreats facing the U.S., but it's not a war—yet," *Computerworld*, 7 April 2010, http://www.computerworld.com/s/article/9174558/After_Google_China_dust_up_cyberwar_emerges_as_a_threat.

Retaliatory Deterrence in Cyberspace

Eric Sterner

The view that deterrence is of little value in securing the nation's information infrastructure is based on a Cold War model of strategic nuclear deterrence. If one examines other approaches to preventing attack, however, deterrence may make significant contributions to US security in cyberspace. Success, however, will require a new mind-set and changed expectations.

Deterrence is ingrained in US national security posture. It dominated Cold War debates and thinking about preventing Soviet aggression against vital US national interests. The lack of a direct US–Soviet war seemed to confirm its utility. Indeed, with the collapse of Soviet communism, deterrence advocates continued to proclaim its primary value in preventing aggression by lesser threats. In 1996, then-secretary of defense William Perry asserted, "And if these powers [rogue states] should ever pose a threat, our ability to retaliate with an overwhelming nuclear response will serve as a deterrent. Deterrence has protected us from the established nuclear arsenals for decades, and it will continue to protect us."[1] Yet, more than two decades into the information age, US policymakers are still working through its applicability in cyberspace. This article first examines cyber vulnerabilities then moves to cyberdeterrence alternatives. Finally it proposes a cyberdeterrent posture and policy.

Cyberspace: Vulnerabilities and Conflict

For the better part of two decades, analysts have recognized, and feared, the new national vulnerabilities that the information revolution created

---

Eric Sterner is a fellow at the George C. Marshall Institute, Washington, DC. He held senior staff positions at the House Armed Services and Science Committees and served in the Office of the Secretary of Defense and as NASA's associate administrator for policy and planning. He has written for several journals, including *Comparative Strategy*, *Washington Quarterly*, and the *Journal of International Security Affairs*. He is a graduate of the American University and the George Washington University.

The author would like to thank the Critical Infrastructure Protection Program of George Mason University's School of Law for sponsoring earlier work on deterrence in cyberspace, and Tim Clancy, Michelle Van Cleave, and Jeff Kueter for their comments on earlier drafts.

for the United States. In 1991, a landmark National Research Council (NRC) study concluded:

> We are at risk. Increasingly, America depends on computers. They control power delivery, communications, aviation, and financial services. They are used to store vital information, from medical records to business plans to criminal records. Although we trust them, they are vulnerable—to the effects of poor design and insufficient quality control, to accident, and perhaps most alarmingly, to deliberate attack. The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb.[2]

If anything, the NRC underestimated the scope of the vulnerability. Computers and the networks that link them have only become more crucial to the functions of a twenty-first-century economy. Systemic infrastructure failures have already been attributed to problems in information networks. The Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack began life to examine a unique kind of nuclear effect. In doing so, it identified a common vulnerability across multiple national infrastructures, namely the proliferation and integration of systems controlled by networked computer chips through the use of embedded supervisory control and data acquisition (SCADA) systems, digital control systems (DCS), and programmable logic controller (PLC) systems.[3] All are vulnerable to electromagnetic pulse in one way or another. More importantly, they represent nodes in cyberspace (not all networks are connected to one another, but the trend is toward greater interconnectivity). Collectively, they represent a massive national vulnerability.

As the NRC predicted, malicious actors ranging from criminals and miscreants to terrorists and nation-states have exploited cyberspace vulnerability for a wide range of purposes. Attacks on commercial systems are a daily occurrence, and it is rare for more than a few days to pass before some company announces it has been attacked. Of late, Google and the instant messaging service Twitter are among the most well-known victims, but their stories are common.[4] A recent survey by the security firm Symantec found that 75 percent of corporate respondents had been attacked in the prior 12 months, and 41 percent of those attacks had been somewhat or highly effective. One hundred percent of respondents admitted to experiencing cyber losses in 2009.[5] One estimate puts 2008 global losses from cyber crime at $1 trillion.[6]

There is a temptation to view such activities as private matters, more suitable for law enforcement than national security. After all, the victims

are commercial entities, and the losses inflicted are nominally private losses. Gross damage to a private entity may be comparable to operating in a known flood plain, hurricane zone, or earthquake-prone area during a natural disaster. In other words, attacks and losses are viewed as the "cost of doing business."

Unfortunately, the vulnerabilities go well beyond simple private losses. They have the potential to affect the entire country. Demonstrating the vulnerability of critical infrastructure to attacks through cyberspace, the US government tested the ability to attack the electrical grid and successfully destroyed an electric generator by hacking a replica of a power plant's control systems.[7] Press reports suggest that power grids in the United States and elsewhere have been penetrated by malicious foreign actors who have done real damage, causing blackouts in multiple cities.[8]

Indeed, the world is awash in cyber conflicts. At least three high-profile international conflicts have been reasonably well- and widely documented: the Israeli-Palestinian conflict of 2000, the Russo-Estonian conflict of 2007, and the Russo-Georgian conflict of 2008.[9] These are not isolated instances. Cyber attacks for ostensibly political purposes occur routinely. They may or may not involve governments. The United States and South Korea were both struck almost simultaneously by several waves of cyber attacks in the summer of 2009.[10] Attacks on Google's Chinese services clearly had political overtones, and Chinese-origin attacks are quite common around the world.[11] There are even signs of ongoing cyber conflicts between al-Qaeda and some of its Islamic opponents as well as a sectarian cyber conflict in the Persian Gulf.[12]

It does not come as a surprise that the United States, as the lone superpower, would find itself on the receiving end of such attacks. In 2007, the Department of Defense identified 43,880 malicious attacks against itself, rising to 54,640 in 2008, and 43,785 just through the first half of 2009.[13] The defense secretary's unclassified e-mail account was breached, and department officials report hundreds of thousands of cyber probes each day. Additionally, in 2007, NASA and the Departments of State, Homeland Security, and Commerce all reported major intrusions resulting in lost data and interrupted operations.[14]

Quite simply, the United States is already engaged in conflict in cyberspace and has been for years. Gen James Cartwright, then-commander of US Strategic Command, testified before the Senate Armed Services Committee:

> However, not unlike the targets of pirates or train robbers of the past, *America is under widespread attack in cyberspace*. Our freedom to use cyberspace is threatened by the actions of criminals, terrorists, and nations alike. Each seeks their own form of unique advantage, be it financial, political, or military, but together they threaten our freedom to embrace the opportunity offered by a globally connected and flattened world. The magnitude of cost, in terms of real dollars dedicated to defensive measures, lost intellectual capital and fraud cannot be overestimated, making these attacks a matter of great national interest. Unlike the air, land and sea domains, we lack dominance in cyberspace and could grow increasingly vulnerable if we do not fundamentally change how we view this battle-space (emphasis added).[15]

More recently, the former director of national intelligence, VADM Mike McConnell, who also served as director of the National Security Agency, stated quite bluntly, "The United States is fighting a cyber-war today, and we are losing."[16]

Deterrence and Cyberspace

The United States has responded to cyberspace as a national security domain in a variety of ways, primarily through improved defense and closer public-private cooperation and coordination. Nevertheless, as fundamental as deterrence is in US national security policy, it is not always clear how it relates to cyberspace. Many focus on the challenges of preventing attacks on or through cyberspace and are skeptical about the prospects for deterrence to contribute to this goal.

Their reasons are straightforward. It becomes quickly apparent that traditional models of deterrence have little relevance to cyberspace. Strategic nuclear deterrence theory, for example, largely presumes a stable bipolar relationship between nation-states of roughly equal power (made so by the possession of nuclear weapons) that share similar expectations and seek to avoid nuclear warfare at all costs, as it threatens each state's supreme interest in its own survival. Theoretically, these nation-states possess the perception and communication skills needed to manage a crisis successfully and avoid the worst possible outcomes. Acknowledging that reality fell well short of the abstract concept, Western policymakers sought to promote deterrence by addressing shortfalls in these key ingredients through force structure, arms control, improved decision making, and better communication links. Thus, deterrence was elevated from a tactic in international relations, to a strategy, to a means of cooperatively managing the superpower

relationship.[17] The concept was so well enshrined in Western strategic culture that some scholars even advocated—or at least argued for tolerating—the modest proliferation of nuclear weapons, whose destructive capabilities theoretically leveled the relative power imbalance, induced a particular clarity in decision making, and otherwise increased peaceful stability in the international system.[18]

Setting aside powerful critiques of strategic nuclear deterrence, none of the elements that purportedly made it successful are present in cyberspace. The number of actors possessing nuclear weapons has been historically low; only nation-states possessed the wherewithal to develop such capabilities. By contrast, the number of actors in cyberspace is astronomically high, growing rapidly, and constantly changing in character, thereby undermining stability, communication, and clarity.[19] Indeed, one might view cyber actors as a threat cloud, constantly evolving and changing shape.

Rather than symmetrical bipolar relationships, cyberspace is governed by a potentially infinite number of asymmetrical, multilateral, and bilateral relationships that are constantly in flux. Stakes, interests, power, and defenses all vary, while ambiguity will be prevalent before, during, and after engagements.

Perhaps the greatest problem encountered when applying strategic deterrence models to cyberspace is the difficulty of identifying the challenger and appropriate retaliatory targets. This was not a problem in traditional models of deterrence, whether nuclear or conventional. Theoretically, an attacker's identity would always be known; only nation-states possessed the capability of launching significant military attacks. Actors in cyberspace, however, are "created" in cyberspace. They may or may not correspond to the creator's identity in the real world. The legal, political, economic, and geographic characteristics that describe an actor in the physical world are not constraining in cyberspace. Worse, a cyberspace actor may not be persistent. It may be created and exist for the short time necessary to launch an attack, only to be quickly discarded after the fact. Thus, if one is to retaliate against a cyberspace actor in the physical domain—where retaliatory options historically lie—by legal, political, economic, or military means, one must first establish connections between the cyberspace actor and his or her physical-world counterpart. For many, this so-called attribution problem is insurmountable. Also, if the cyber attacker is not a nation-state, retaliation may involve impinging on the sovereignty of the country in which the cyber attacker is physically located or of the country(ies) through which the attack was launched. Thus, retaliation has

a high likelihood of collateral damage. In some cases, a challenger might launch an attack simply to provoke retaliation to advance some other political interest. In such cases, the threat of retaliation might actually invite the attack!

Alternatives to Deterrence

Left with few retaliatory options, the defender can only hope to ensure that its defenses are better than the challenger's offenses and take steps to manage the risks and consequences of losing the offense-defense interaction. Martin Libicki, who thoroughly analyzed cyberdeterrence and found it wanting, recommended an approach akin to safety engineering.[20] More recently, Greg Rattray noted parallels between public health and cyber security and suggested drawing from public health risk-management models to help secure cyberspace.[21] Because cyberspace is not defined nationally, it is necessary to improve its overall resistance to malicious behavior and, in so doing, improve the US defense posture. Rattray recommends improving partner security capacity and capabilities, engaging and supporting multi-stakeholder international organizations, and encouraging network operator groups to play active roles in making systems more resistant to attack. He concludes: "The United States should take lessons from public health efforts at national and global levels. Specifically, the federal government should support public-private collaboration that enables early warning of new threats, rapid response to contain the spread of malware, and long-term commitment to eradicating the malicious activity that often thrives in the cyber commons."[22]

Ultimately, resilience and flexibility become key for defense. It absolutely is necessary to improve the resiliency of cyberspace writ large, not to mention our own use of it, and our flexibility to deal with attacks—successful or otherwise—to improve our posture in an offense-defense interaction. Moreover, managing and minimizing the risks and consequences of an attack may dissuade some attackers by denying them the object of their attack. Deterrence by denial is a well-accepted posture. In the end, risk- and consequence-management policies will help allocate resources more efficiently than the ad hoc approach used now. In many ways, they will remain the main line of security in cyberspace after straightforward defense. Nevertheless, their limitation lies in the fact that they divorce cyber security from cyber conflict and the attack from the attacker.

Conflict involves interaction between conscious actors, each of which behaves in a way intended to defeat the other relative to the stakes of their conflict. Each will employ a strategy it thinks will advance its goals. Viruses, worms, safety flaws, and the like are not willful; they certainly do not employ conscious strategies for the purposes of defeating their victims. Rather, they are merely tools reflecting the intent and capabilities of an attacker or the vulnerabilities of a defender.

A risk/consequence–management policy framework pays less attention to threats as a function of intent and capability. Therefore, it may blind the defense to sudden changes in the nature of the threat, either in terms of general attitudes toward the United States or the particular goals and stakes of a specific engagement or campaign. It may also create a class of malicious behavior for which we are unprepared to hold actors responsible, with a new set of tools to employ against US national interests in conjunction with more traditional geopolitical maneuvers. Separating the attack from the intent of the attacker begins to break down the fundamental ingredients of a successful campaign. Defense shifts from an interaction between belligerents to an interaction of weapons. Of course, one cannot prevail in a cyber conflict any more than a conflict in other domains if one only thinks about it at this level.

This is a crucial challenge. Dominant modes of analysis seek to segment threats into a variety of categories based on a mix of factors, usually including the actor's physical description (criminal, nation-state, corporation), motives (criminal, harassment, political, strategic), target, and consequences of the attack.[23] Risk management ultimately focuses on the highest-risk challenges and may pay less attention to lower-level threats, such as criminal activity, or those primarily affecting private persons. Unfortunately, ambiguity in cyberspace creates incentives and opportunities for one kind of attacker to disguise itself and its motive for an attack. It also means that what appears to be one kind of attack may, in fact, be a particular tactic in another. For example, states may use front groups to assemble botnets which they rent out for criminal activity and use to launch distributed denial-of-service attacks as a distraction for something more decisive elsewhere. An activist may simply find itself the covert recipient of sufficient government funds to "rent" cyberspace weapons and launch harassment attacks. In other words, intentions and capabilities are subject to rapid change. Yesterday's criminal threat is tomorrow's strategic attack. With that in mind, it behooves a defender to pay excruciatingly

close attention to such dynamics lest it miss the suddenness with which a cyberspace threat to its security might arise.

Finally, too heavy an emphasis on a risk-management approach largely cedes the initiative to a challenger. Because it is focused on reducing vulnerabilities and minimizing consequences, it is largely reactive to a specific attack or campaign. A conflict typically involves both defense and offense, even if the offense is limited to counterattacks. Without imposing the consequences of a counterattack—strategic, operational, or tactical—on an attacker, the defender is merely taking a beating.

An Alternative Model

The limits of risk management and the offense-defense interaction return one to the discussion of deterrence. Its perceived limitations, however, are drawn from analysis of our Cold War experience with strategic nuclear warfare. As it turns out, much of this analysis used the wrong deterrence model.

Many treated Cold War strategic deterrence as a binary switch: deterrence prevents conflict; if a conflict breaks out, deterrence has failed. In 2001, Secretary of Defense Donald Rumsfeld restated the point in his forward to the *Quadrennial Defense Review Report*: "The strategy that results is built around four key goals . . . [including] decisively defeating any adversary if deterrence fails."[24] This view may be a relic from theories associated with nuclear weapons. Taking state survival as paramount, theorists concluded that nuclear war was always unacceptable and, therefore, to be avoided at all costs.

As discussed earlier, cyberspace, and American interests in it, are already under attack. Conflicts within cyberspace are continual, with relative peaks and valleys in the intensity of their connection to politics. A deterrence model that focuses on the prevention of armed conflict will thus fall short—the conflict is already underway. In the end, it may not be that deterrence falls short in cyberspace; merely that the deterrence model against which most analysts measure the cyber conflict problem falls short.

The chairman of the Joint Chiefs of Staff, ADM Michael Mullen, noted that US deterrence theory had not appreciably improved in 20 years and concluded, "We need a new model for deterrence theory, and we need it now. . . . We need to be ready—actually and completely—to deter a wide range of new threats. It is not just about cleaning someone else's clock

anymore. We need a new model of deterrence that helps us bring our own clock up to speed with the pace and the scope of the challenges of this new century."[25] Indeed, more than one model will be necessary. The need is particularly acute in cyberspace.

The role deterrence can play in shaping, containing, or even preventing a continuation of ongoing conflict is intuitive but often ignored in analyses of deterrence in cyberspace. During Operation Desert Storm, for example, US policymakers signaled clearly enough to Iraqi leaders that the United States could respond to Iraq's use of weapons of mass destruction by escalating its war aims to include regime change.[26]

More generally, deterrence threats can be used to affect a challenger's choices of means and aims in a conflict. Throughout its history, Israel has sought to deter attacks from nonstate actors by changing the nature of its conflict with those actors. It countered cross-border Palestinian raids, for example, by threatening and conducting retaliatory attacks against Jordan and Egypt, each of which had greater reason to fear Israeli retaliatory threats and possessed capabilities to threaten and punish Palestinian raiders.[27] In other words, Israel combined threats and actions to change the nature of the conflict in an attempt to create a better situation for itself. This "active deterrence" reflected a combination of the actual use of force and threats of force to achieve its security goals. Doron Almog offers an updated concept, dubbing it "cumulative deterrence." For him, "cumulative deterrence is based on the simultaneous use of threats and military force over the course of an extended period of conflict."[28] Israel's readiness to change the strategic dynamic of a conflict if necessary by escalating it horizontally or vertically has established a deterrent posture that effectively prevents some attacks and contains the dynamics of conflicts within certain boundaries. Consequently, Israel is able to wage conflicts on more-favorable terms that have the potential to limit the conflict and, ideally, bring peace. Unlike nuclear deterrence, which focuses on preventing conflict, these concepts revolve around shaping it over time.

Might such a posture be more appropriate for cyberspace? Certainly it suggests there is less reason for despair about deterrence than some have assumed. Of course it involves changing expectations. Law enforcement accepts imperfect deterrence as the nature of the beast rather than dismissing the concept entirely. The same can be said for cyberspace. Resigned admonitions to avoid overwrought strategic metaphors for security in cyberspace and instead approach threats by ascribing to defense the more pedes-

trian status of "safety engineering" are well heeded, but they should not become an excuse for forgoing deterrent options. Instead, it will be necessary to view cyberspace attackers as thinking beings who engage in some form of cost-benefit calculus and then seek to change that estimation in their minds. Deterrence in cyberspace will be far from perfect, but it is also far from hopeless.

Toward a Cyberdeterrent Posture and Policy

In moving toward a cyberdeterrent posture, the United States will need to change the strategic dynamic of the conflict. It will not be effective simply to meet challengers on their terms, at the times and places of their choosing. Doing so cedes the initiative, gives them an opportunity to continually probe and identify vulnerabilities, and enables them in advance to lay out lines of retreat from an engagement should the offense-defense interaction go badly.

First and foremost, the United States must retaliate for malicious cyber behavior. Today, US officials often consider punishing cyber aggressors through domestic law enforcement, largely because those means are readily available. Such tools are entirely inadequate. Domestic statutes regarding cyber crimes typically: (1) require prosecutors to attribute a monetary value to the damage inflicted, which may be irrelevant or inappropriate for national security matters; (2) utilize high evidentiary standards associated with criminal prosecution and its presumption of innocence; and (3) assume that a criminal defendant can be made to stand trial.[29] As a practical matter, these tests cannot reliably be met in cyber attacks that cross territorial boundaries, they are inadequate for dealing with harassing attacks or those that share traits with espionage, and they are inappropriate for dealing with state-sponsored or state-sanctioned cyberspace attacks. Moreover, such retaliation is extraordinarily slow with an extremely low likelihood of execution. Indeed, successful prosecutions are still remarkable events, largely because they are so rare relative to the scale of attacks.

Other retaliatory options will be needed. Political, economic, and military means must be explored. While usually considered in the context of state-to-state relationships, these methods have been used against nonstate actors for a variety of purposes, including advancing nonproliferation agendas and fighting the global war on terror. In the case of political and economic retaliation, the threshold needed to justify imposing sanctions

should be lower, usually left to the discretion of the president once he is confident that certain conditions have been met.

Kinetic and cyber retaliation are more problematic, due in part to questions of proportionality, collateral damage, and attribution. Kinetic measures may be precise but generally not precise enough to get the NRC's proverbial terrorist-with-a-keyboard without doing considerable collateral damage. Moreover, it can be argued that the prospect of taking life in a kinetic attack far outweighs the damage one can commit with a cyber attack; that is, it is disproportional. Richard Harknett summed up the dilemma:

> At its core, deterrence theory rests on the principle of retaliation in kind, where the cost inflicted in retaliation will at least match the level of costs associated with the offensive attack. If an attack reduces no buildings to rubble and kills no one directly, but destroys information, what is the response? We tend to think about information as intangible, but the loss of information can have tangible personal, institutional, and societal costs. What credibly can be placed at risk that would dissuade a state from contemplating such an attack?[30]

The dilemma is more simply framed as a "bits-for-lives" trade-off, in which the value placed on the challenger's life is always higher than the value placed on the defender's bits. Presumably, the United States values lives more than bits, so any retaliatory threats are not credible. Framing the dilemma in this manner is too limiting.

The United States has employed military measures in cases where its values, interests, and international prerogatives were at stake but its national survival was not. In the 1980s, it used force in Grenada and Panama because US citizens were threatened. In the 1980s and 1990s, it used force against Libya in retaliation for terrorist attacks in Europe; in the Persian Gulf to preserve the global flow of oil; in Lebanon, Somalia, and Haiti for peacekeeping and humanitarian reasons; and in the Balkans to prevent ethnic cleansing. Thus, the threat of force in retaliation for cyber attacks that adversely affected vital national interests in some meaningful way seems eminently credible, the concern over trading lives for bits notwithstanding. Certainly, the United States possesses the ability and has demonstrated the will to use force in instances that fall well below the threshold of national survival. Thus, if—and this is a big "if"—the United States can identify an attacker with enough confidence to permit retaliation, military options should be available.

Questions of proportionality go well beyond a lives-for-bits trade-off. Traditionally, the concept is drawn from theories of justice, whether in

war or the legal system. The punishment should fit the crime, as it were, and every military provocation should not necessitate a massive response. That said, in and of itself, cyber conflict lies somewhere between the two. It may not rise to the level of warfare, but the legal system is often inadequate to deal with it as a strategic tool in international relations. Meanwhile, small attacks of modest intent may have immense consequences, even perhaps inadvertently, as they propagate through global networks. Conversely, massive attacks of aggressive intent may have modest consequences, particularly if they are poorly executed or the target has effectively defended against them and/or taken steps to minimize the damage. Thus, concepts of proportionality drawn from other domains are out of place. Policymakers will ultimately have to decide what constitutes a proportional response on a virtual case-by-case basis, taking into account a variety of factors ranging from the attacker's intent, consequences of the attack, and confidence levels in identifying responsible parties to the strategic situation, concerns about repeat attacks, and available retaliatory options. Many of these judgments will have to be incorporated into rules of engagement to enable the defenders of cyberspace engaged in the conflict to make decisions about counterattacks, just as police and soldiers in the field are trusted with judgments about the use of lethal force.

There appears to be an unwritten assumption that knowing the physical-world identity of a cyber attacker is a prerequisite to retaliation. This is eminently reasonable when one's primary retaliatory tools were designed for attackers in the physical world. But, the challenge of cyberspace—that it is not limited by the physical world (even if it does not exist independent of the physical world)—also represents an opportunity. Instead of trying to fit the square pegs of retaliatory options developed for the physical world into the round holes of cyberspace, the United States needs to develop and employ policies, doctrine, tools, deterrent models, and rules of engagement for cyber retaliation against actors in cyberspace. In other words, it needs the ability to retaliate against cyber attackers without necessarily knowing who they are in the physical domain.

The challenge of identifying retaliatory targets remains. Attribution, however, is not an insurmountable problem. Many factors come into play. First, technical tools for identifying sources of cyber aggression are constantly improving. In studying an attack or the creation of offensive cyber capabilities, it is often possible to identify e-mail accounts, Internet service providers, and even servers from which certain kinds of behavior emanate.

Joseph Menn recently documented the efforts of a private security expert working with British and Russian law enforcement to track the online behavior of criminal gangs and defeat their attacks on private web business. In particular, he noted the success of nongovernment groups and individuals in building thorough profiles of malicious cyber actors, sometimes even tying them to their counterparts in the physical domain.[31] According to public reports, researchers identified websites during the Russo-Georgian cyber conflict of 2008 hosting downloadable "weapons," traced activities to computers known to be controlled by Russian organized crime, and linked related Internet traffic to servers controlled by Russian telecommunications firms.[32] Islamist websites contain instructions and links to means of cyber attack.[33] One such site, Al-jinan.org, offered downloadable software to attack a preapproved list of Internet protocol addresses and a simple Windows interface that enables the visitors to conduct attacks at their leisure, based in part on the speed of their connection to the Internet.[34] Some ostensibly legitimate businesses are even selling "hacks" and other software vulnerabilities to the highest bidder.[35] In short, in some significant cases it is possible to identify specific sources of cyber attack.

Secondly, strategic context matters. The Russo-Estonian cyber conflict did not occur in a vacuum but in the context of an ethnic dispute inside Estonia, to which Russia became a party. Similarly, the Russo-Georgian cyber conflict occurred against the backdrop of a physical invasion of the latter. This is not to suggest that an underlying strategic situation will definitively identify an attacker. Indeed, criminals may be motivated to take advantage of international crises; states engaged in a type of attrition cyber attack may engage in most activity at relatively peaceful times so as not to exacerbate a political conflict; and, third parties may well seek to disguise their activities to create a political crisis between two other parties. Nevertheless, policymakers should consider the strategic situation both in assessing an attack and executing retaliatory options. That context will contribute to confidence levels in attributing an attack and selecting a particular means of punishing an aggressor.

Thirdly, the United States can hold third parties accountable commensurate with their role in enabling or allowing cyber attacks that do it harm. Unlike other conflict domains (sea, air, land, and space), cyberspace is a created medium. Someone owns the servers, nodes, transmission lines, and infrastructure that create cyberspace and enable it to function. Arguably,

today we have established a norm of irresponsibility that holds these owners and creators harmless for third-party damages done by, with, or through the things they create. Establishing a deterrent will require defenders to put cyberspace creators on notice that they will be held accountable for use of their creation. Such an approach need not be always adversarial. More often than not, the interests of the government in deterring attacks will coincide with the interests of cyberspace creators in preserving the value and utility of their creation. For example, in 2008, while investigating a web-hosting firm engaged in suspicious activity, reporters from the *Washington Post* approached the enterprise running the server farm on which the hosting company had based its business. Shortly thereafter, the server farm disconnected the web-hosting company from its servers, and security experts noted a significant drop in global spam activity.[36] Should cooperative efforts fail, however, escalating horizontally to the creators of cyberspace will change their interests such that they use the leverage they have over the users of their infrastructure to constrain attacks.

The United States might start down this path by putting cyberspace actors on notice that it will hold them accountable for how their creation is used, perhaps by creating blacklists of bad actors who consistently tolerate malicious cyber attacks over or through their infrastructure. Persistent toleration of such attacks may become sufficient grounds for some form of retaliation by political, economic, cyber, or kinetic means.

It will be tempting to draw "redlines" and clarify what kinds of malicious behavior one is attempting to deter. One might understandably focus on deterring some sort of cyber Pearl Harbor or other nightmare scenario that involves widespread economic damage. Of course, clear redlines signal that malicious activity falling below that threshold is of less concern, inviting attackers to continue their efforts there. Rather than drawing specific redlines, the United States needs to consider a range of retaliatory options to use against a range of threats that it may not be able to rank hierarchically, given the speed with which threats might change. Thus, cyber attacks should be no more tolerable than major attacks on strategic infrastructure. Neither gets a "pass," as it were. If there is a parallel in the physical domain, the concept of "broken window" law enforcement comes to mind. By stopping small infractions, one creates a cumulative effect that deters bad actors from escalating to more serious behavior.[37]

Over time, a commitment to retaliation for cyber attacks by a variety of means (political, economic, military, or cyber) and a willingness to hold

cyberspace creators accountable for their role in permitting or enabling attacks will create a deterrent posture. By no means will the United States be able to retaliate for every attack, but visible retaliation will create risk for potential attackers, affecting their cost-benefit analysis. Those cyberspace actors contemplating attacks on the United States will have to consider the potential punishment that such an attack might invite. Similarly, those who own and maintain the infrastructure of cyberspace will have to weigh the risks of allowing their infrastructure to be used at will by various cyberspace attackers. Presumably, at least a portion of them will improve their situational awareness and be more accommodating to cyberspace defenders, lest they become retaliatory targets themselves.

The United States cannot adopt such a posture tomorrow or simply through declaratory statements. It will require sophisticated rules of engagement, careful mapping of global cyber networks to better anticipate secondary or tertiary consequences, accelerated development of advanced forensic tools, and improved retaliatory capabilities, ranging from cyber weapons and limited war plans to presidential sanction authority and international cooperation to identify cyber attackers and the legal means of punishing them. Careful study of the potential unintended consequences will be necessary. Finally, it will take a series of visible retaliatory actions—political, economic, military, and cyber—over time to create a reasonable, if not certain, expectation of the risk of punishment for potential attackers. These specific measures go well beyond the scope of this article. Moreover, developing these tools may take years, while the cyber threat is here now.

Conclusion

Conflict in cyberspace does not fall squarely within the bounds of law enforcement or traditional warfare. As a unique environment with unique actors, power distributions, and interests, it represents something else entirely. With that in mind, it is necessary to develop new intellectual frameworks for understanding cyber conflict and securing US interests. Simply importing concepts and thought processes from other domains will prove entirely inadequate. Strategic nuclear deterrence is unique to a nuclear environment; indeed, it may well be unique to the Cold War.[38] It does not represent a useful posture for cyberspace. That does not mean deterrence has no value. A more forward-leaning posture that incorporates the realities of cyberspace is necessary.

To be sure, the deterrent posture laid out herein may be controversial. It should be. An immense amount of study, analysis, and additional work is needed to understand the dynamics of cyber conflict, how different retaliatory options might affect attackers, the most useful means of holding an attack's enablers accountable, escalatory ladders, authorities, roles, and missions. Moreover, Americans are reluctant to escalate conflicts vertically or horizontally. Although the United States has done so in the past, holding third parties responsible for their toleration or enabling of bad actors adds risk to any given conflict. Nevertheless, the alternatives are insufficient. Risk management, consequence management, and the offense-defense interaction create a policymaking framework that may cede the initiative to attackers. Given the stakes involved for the United States, policymakers must explore all measures available to improve US security. Deterrence in cyberspace will not become a first, second, or even third line of defense. Risk and consequence management and the improvement of defenses at the point of attack are likely to long dominate US security in cyberspace. But, deterrence may yet contribute to security by helping contain the severity and frequency of attacks and focusing attention on cyber conflict as the interaction of conscious actors whose decision-making processes can be influenced. SSQ

Notes

1. Quoted in Keith Payne, *The Fallacies of Cold War Deterrence and a New Direction* (Lexington: University Press of Kentucky, 2001), 82.

2. National Research Council, *Computers at Risk: Safe Computing in the Information Age* (Washington: National Academies Press, 1991), 7.

3. Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, *Critical National Infrastructures Report*, April 2008, 1–16, http://www.empcommission.org/docs/A2473-EMP_Commission-7MB.pdf.

4. Jessica Vascellaro, "Hackers Briefly Bring Down Twitter," *Wall Street Journal*, 18 December 2009; Nik Cubrilovic, "The Anatomy Of The Twitter Attack," *TechCrunch.com*, 19 July 2009; and Siobhan Gorman and Jessica Vascellaro, "Google Attack Linked to Asian Hackers," *Wall Street Journal*, 22 February 2010, http://online.wsj.com/article/SB10001424052748704751304575080362745174130.html?mod=WSJ_hpp_MIDDLTopStories.

5. Symantec, *State of Enterprise Security, 2010*, http://www.symantec.com/content/en/us/about/presskits/SES_report_Feb2010.pdf. Another security company, McAfee, sponsored a Center for Strategic and International Studies (CSIS) survey report, *In the Crossfire: Critical Infrastructure in the Age of Cyber War*, which revealed similar findings.

6. David Z. Bodenheimer, *Statement Before the House Armed Service Committee's Subcommittee on Terrorism, Unconventional Threats and Capabilities Concerning Private Sector Perspectives on Department of Defense Information Technology and Cybersecurity Activities,* 10 February 2010, 4.

7. Jeanne Meserve, "Sources: Staged cyber attack reveals vulnerability in power grid," *CNN*, 26 September 2007, http://www.cnn.com/2007/US/09/26/power.at.risk/index.html; and Glenn Derene, "How Vulnerable is U.S. Infrastructure to a Major Cyber Attack?" *Popular Mechanics*, October 2009, http://www.popularmechanics.com/print-this/4307521.

8. Siobhan Gorman, "Electricity Grid in U.S. Penetrated by Spies," *Wall Street Journal*, 8 April 2009; Michael Mylrea, "Brazil's Next Battlefield: Cyberspace," *Foreign Policy Journal*, 15 November 2009, http://www.foreignpolicyjournal.com/2009/11/15/brazils-next-battlefield-cyberspace; and Tom Espiner, "CIA: Cyber attack caused multiple-city blackout," *c/net news*.com, 22 January 2007, http://www.news.com/CIA-Cyber attack-caused-multiple-city-blackout/2100-7349_3-6227090.html.

9. For a discussion, see Col Patrick Allen and Lt Col Chris Demchak, "The Palestinian-Israeli Cyberwar," *Military Review*, March–April 2003; Brian Krebs, "Report: Russian Hacker Forums Fueled Georgia Cyber Attacks," *Washington Post*, 17 October 2008, http://voices.washingtonpost.com/securityfix/2008/10/report_russian_hacker_forums_f.html?hpid=sec-tech; Stephen W. Korns and Joshua E. Kastenberg, "Georgia's Cyber Left Hook," *Parameters* 38, no. 4 (Winter 2008/2009): 60–76; Eneken Tikk et al., *Cyber Attacks against Georgia: Legal Lessons Identified* (Talinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, August 2008); Joshua Davis, "Hackers Take Down the Most Wired County in Europe," *Wired Magazine*, issue 15.09 (21 August 2007); and Richard A. Clarke and Robert K. Knake, *Cyber War* (New York: HarperCollins, 2010). Given the strategic context and manner in which the attacks unfolded, circumstantial evidence suggests that governments may have colluded in the attacks, although such collusion may not have been necessary for attacks to take place.

10. John Sudworth, "New 'cyber attacks' hit S. Korea," *BBC News*, 9 July 2009, http://news.bbc.co.uk/2/hi/asia-pacific/8142282.stm; and James A. Lewis, "The 'Korean' Cyber Attacks and their Implications for Cyber Conflict," Center for Strategic and International Studies, October 2009.

11. Bryan Krekel et al., "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation," prepared for US–China Economic and Security Review Commission, 9 October 2009.

12. Ellen Knickmeyer, "Al-Qaeda Web Forums Abruptly Taken Offline," *Washington Post*, 18 October 2008, A-01.

13. US–China Economic and Security Review Commission, *2009 Report to Congress* (Washington: US–China Economic and Security Review Commission, November 2009), 68.

14. CSIS, *Securing Cyberspace for the 44th Presidency* (Washington: CSIS, December 2008), 12–13.

15. Gen James Cartwright, USMC, *Statement Before the Strategic Forces Subcommittee, Senate Armed Services Committee*, 28 March 2007, 4–5.

16. Mike McConnell, "To win the cyber-war, look to the Cold War," *Washington Post*, 28 February 2010, B-01.

17. See, for example, Patrick Morgan, *Deterrence Now* (Cambridge, UK: Cambridge University Press, 2003), chap. 1. The logic of deterrence, as well as its flaws, is considerably more complex than this. Other factors such as psychology, cognition, certainty of retaliation, offense-dominance, and the like come into play. Developed in the context of strategic nuclear deterrence, each of these factors also, arguably, limits the utility of traditional concepts of deterrence in cyberspace.

18. See Kenneth Waltz, "More May Be Better," in *The Spread of Nuclear Weapons: A Debate*, eds. Scott D. Sagan and Kenneth Waltz (New York: W. W. Norton & Company, 1995); Martin van Creveld, *Nuclear Proliferation and the Future of Conflict* (New York: Free Press, 1993); Devin Hagerty, "Nuclear Deterrence in South Asia: The 1990 Indo-Pakistani Crisis," *International Security* 20, no. 3 (Winter 1995/96); and John Mearsheimer, "Back to the Future: Instability in Europe after the Cold War," in *The Perils of Anarchy: Contemporary Realism and International Security*, eds. Michael Brown, Sean Lynn-Jones, and Steven Miller (Cambridge, MA: MIT Press, 1995).

19. Some estimates indicate the number of Internet users rose from roughly 360 million in 2000 to 1.8 billion by 2010. See http://www.internetworldstats.com/stats.htm.

20. Martin Libicki, *Defending Cyberspace and Other Metaphors*, (Washington: National Defense University [NDU] Press, 1997), 41, fn. 1, 107–8. Libicki urges policymakers to adopt a philosophy that will lead "information warfare . . . to acquire the pedestrian status of safety engineering." For a more recent and thorough analysis, see Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009).

21. Greg Rattray, Chris Evans, and Jason Healey, "American Security in the Cyber Commons," in *Contested Commons: The Future of American Power in a Multipolar World*, eds., Abraham Denmark and James Mulvenon (Washington: Center for a New American Security, 2010), chap. 5.

22. Ibid., 167.

23. See David S. Alberts, *Defensive Information Warfare* (Washington: NDU Press, 1996), 22–39; Irving Lachow, "Cyber Terrorism: Menace or Myth," in *Cyberpower and National Security*, eds., Franklin Kramer, Stuart Starr, and Larry Wentz (Washington: NDU Press, 2009), 437–64. Alberts' analysis, while dated, has held up well in subsequent studies.

24. *Quadrennial Defense Review Report* (Washington: DoD, 2001), iii–iv.

25. ADM Michael Mullen, "From the Chairman: It's Time for a New Deterrence Model," *Joint Force Quarterly*, issue 51 (4th Quarter, 2008): 2–3.

26. See James A. Baker III, *The Politics of Diplomacy: Revolution, War & Peace*, 1989–1992 (New York: G. P. Putnam's Sons, 1995), 359. The role of Baker's threat in Iraq's nonuse of weapons of mass destruction remains debated. See, for example, Avigdor Haselkorn, *The Continuing Storm: Iraq, Poisonous Weapons, and Deterrence* (New Haven, CT: Yale University Press, 1999).

27. Jonathan Shimshoni, *Israel and Conventional Deterrence: Border Warfare from 1953 to 1970* (Ithaca, NY: Cornell University Press, 1988).

28. Doron Almog, "Cumulative Deterrence and the War on Terrorism," *Parameters* 34, no. 4 (Winter 2004/2005): 8.

29. See, for example, 18 USC § 1030, "Fraud and Related Activity in Connection with Computers," available from the Department of Justice Computer Crime and Intellectual Property Section, along with relevant sentencing guidelines tied to damages, at http://www.justice.gov/criminal/cybercrime/cclaws.html#fedcode. There is a robust and rapidly growing body of literature on laws relating to cyber conflict, including relevant bodies of international law, the Laws of Armed Conflict, international law, espionage statutes, and criminal and civil codes. For a useful summary discussion of the issues, see *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyber Attack Capabilities* (Washington: National Academies Press, 2009), chap. 7.

30. Richard J. Harknett, "Information Warfare and Deterrence," *Parameters* 26, no. 4 (Autumn 1996): 93–107. Not all deterrence concepts are limited by the need to retaliate in-kind or proportionally. Instead, at its core, deterrence rests on the defender's threat to impose costs on a challenger that exceed the challenger's willingness to pay, at least in the challenger's mind.

31. Joseph Menn, *Fatal System Error* (New York: Public Affairs, 2010).

32. John Markoff, "Before the Gunfire, Cyber Attacks," *New York Times*, 13 August 2008, http://nytimes.com/2008/08/13/technology/13cyberhtml?_r=1&pagewanted=print; Brian Krebs, "Report: Russian Hacker Forums Fueled Georgia Cyber Attacks," *Washington Post*, 17 October 2008, http://voices.washingtonpost.com/securityfix/2008/10/report_russian_hacker_forums_f.html?hpid=sec-tech. See also Tikk et al., *Cyber Attacks against Georgia*.

33. Steve Coll and Susan B. Glasser, "Terrorists Turn to the Web as Base of Operations," *Washington Post*, 7 August 2005, A-01.

34. Larry Greenemeier, "'Electronic Jihad' App Offers Cyberterrorism for the Masses," *InformationWeek*, 2 July 2007.

35. Brian Krebs, "Auction of Software Flaws Stirs Concerns," *Washington Post*, 13 July 2007, D-01, http://www.washingtonpost.com/wp-dyn/content/article/2007/07/12/AR2007071202070_pf.html. As of 14 October 2008, the website for the company was still active and advertising for additional researchers.

36. Brian Krebs, "Major Source of Internet Spam Yanked Offline," *Washington Post*, 12 November 2008, http://www.washingtonpost.com/wp-dyn/content/article/2008/11/12/AR2008111200658_pf.html.

37. George Kelling and James Q. Wilson, "Broken Windows," *Atlantic Monthly*, March 1982, http://www.theatlantic.com/magazine/archive/1982/03/broken-windows/4465/; and Kelling, "'Broken Windows' Works," *Forbes.com*, 16 July 2009, http://www.manhattan-institute.org/html/miarticle.htm?id=5091.

38. For that matter, strategic nuclear deterrence may be unique to the United States. There is evidence that the Soviet Union did not share the concept.

Perspectives for Cyber Strategists on Law for Cyberwar

Charles J. Dunlap Jr., Major General, USAF, Retired

The proliferation of martial rhetoric in connection with the release of thousands of pages of sensitive government documents by the WikiLeaks organization underlines how easily words that have legal meanings can be indiscriminately applied to cyber events in ways that can confuse decision makers and strategists alike.[1] The WikiLeaks phenomenon is but the latest in a series of recent cyber-related incidents—ranging from cyber crises in Estonia and Georgia[2] to reports of the Stuxnet cyberworm allegedly infecting Iranian computers[3]—that have contributed to a growing perception that "cyberwar" is inevitable, if not already underway.[4]

All of this generates a range of legal questions, with popular wisdom being that the law is inadequate or lacking entirely. Lt Gen Keith B. Alexander, the first commander of US Cyber Command, told Congress at his April 2010 confirmation hearings that there was a "mismatch between our technical capabilities to conduct operations and the governing laws and policies."[5] Likewise, Jeffrey Addicott, a highly respected cyber-law authority, asserts that "international laws associated with the use of force are woefully inadequate in terms of addressing the threat of cyberwarfare."[6]

This article takes a somewhat different tact concerning the ability of the law of armed conflict (LOAC) to address cyber issues.[7] Specifically, it argues that while there is certainly room for improvement in some areas, the basic tenets of LOAC are sufficient to address the most important issues of cyberwar. Among other things, this article contends that very often the real difficulty with respect to the law and cyberwar is not any lack of "law," per se, but rather in the complexities that arise in determining the necessary facts which must be applied to the law to render legal judgments.

Prof. Charles J. Dunlap Jr. is associate director of the Center on Law, Ethics, and National Security at Duke Law School and a visiting professor of the practice there. Before retiring as a major general in June 2010 after 34 years of active duty, he served as deputy judge advocate general of the Air Force. He also serves on the board of advisors for the Center for a New American Security.

That is not to say that applying the facts—such as they may be discernable in cyber situations—to a given legal principle is anything but a difficult task. Yet doing so has a direct analogy to the central conundrum faced by military decision makers fighting in more traditional battlespaces—that is, the need to make quick decisions based on imperfect data. Because of the inherent fog of war,[8] commanders gamely accept a degree of uncertainty in the legal advice they receive, just as they tolerate ambiguity inherent in other inputs. Too often it seems as if cyber strategists, schooled in the explicit verities of science, expect a level of assurance in legal matters rivaling mathematical equations. All law, but especially LOAC, necessarily involves subjectivity implicit in human reasoning that may be troubling to those of a technical mind-set accustomed to the precision that their academic discipline so often grants.

This article will not provide cyber strategists with "cookbook" solutions to all the permutations of every legal dilemma cyberwar could produce. Instead it offers some broad legal considerations to facilitate thinking about the role of LOAC in cyberwar and suggests cautions for the military cyber strategist in the future.

Perspectives on the law are expressed here as definitively as possible to counter complaints about indecisiveness of legal analysis. The author chose among differing and even conflicting legal interpretations and theories, and readers should understand that positions in this writing may be disputed by other legal experts. Accordingly, cyber strategists must always seek the advice of legal counsel for guidance in specific situations, especially as law and policy evolve.

Cybersizing LOAC

Discomfort among cyber strategists relying on existing LOAC norms is understandable. After all, most of the international agreements and practices of nation-states that comprise LOAC predate the cyber era. Indeed, many observers believe the need for a new legal regime designed for cyberwar is urgent.[9] Cyber expert Bruce Schneier warns that time is running out to put in place a cyber treaty that could, he advocates, "stipulate a no first use policy, outlaw unaimed weapons, or mandate weapons that self-destruct at the end of hostilities."[10]

However, to paraphrase former Secretary of Defense Donald Rumsfeld, you go to war with the LOAC you have, not the LOAC you may want.

While agreements that might expedite cyber-law enforcement efforts are possible, it is not likely that any new international treaty governing cyberwar or cyber weaponry will be forthcoming in the foreseeable future. To begin with, the utility of such treaties is checkered at best. Although most people cheer international treaties that have banned chemical and biological weapons, some experts see them as unintentionally inhibiting the development of nonlethal and low-lethality weaponry.[11] More generally, pundit Charles Krauthammer gives this scorching analysis: "From the naval treaties of the 1920s to his day, arms control has oscillated between mere symbolism at its best to major harm at its worst, with general uselessness being the norm. The reason is obvious. The problem is never the weapon; it is the nature of the regime controlling the weapon."[12]

The Obama administration also seems guarded with respect to cyber arms agreements. Writing in a recent issue of *Foreign Affairs*, Deputy Secretary of Defense William Lynn observed that "traditional arms control agreements would likely fail to deter cyberattacks because of the challenges of attribution which make the verification of compliance almost impossible."[13]

Even more substantively, nations may perceive the goals of any cyber treaty differently. For example, the Russians have long proposed an international cyber agreement (although couched in terms aimed at "information warfare").[14] However, journalist Tom Gjelten warns that "democracies have reason to proceed cautiously in this area, precisely because of differences in the way cyber 'attacks' are being defined in international forums." The Russians and others see "ideological aggression" as a key cyberwar evil and appear to be seeking an agreement that assists government censorship of the Internet and bans outside countries from supporting the cyber efforts of dissidents.[15]

Gjelten notes that at a 2009 meeting to discuss the Russian proposals, the "U.S. delegation declared that existing international law could theoretically be applied to cyber conflict and that the United States would support the establishment of 'norms of behavior' that like-minded states could agree to follow in cyberspace."[16] American cyber strategists, however, should remain cautious of even that modest initiative. As attractive as it may be to have more clarity as to what the international community considers, for example, as an "act of war" in cyberspace, once an international norm is established, it forever after can be a legal impediment. If, as Gjelten argues, the United States has the most advanced cyberwar capability,

any new agreement or norm would likely oblige it to "accept deep constraints on its use of cyber weapons and techniques."[17]

The "Act of War" Conundrum

As already suggested, of all the legal issues bedeviling cyber strategists, the issue of when a cyber event amounts to an act of war seems to capture the most interest.[18] This is not a new query but one that is critical because its resolution can define the options available to decision makers. If it is truly "war," then a response under a national-security legal regime is possible; if not, then treating the matter as a law enforcement issue is appropriate. This is a distinction with a difference.[19]

A national-security legal regime is one where LOAC largely governs, while the law enforcement model essentially employs the jurisprudence of criminal law. The former is inclined to think in terms of eliminating threats through the use of force; the latter uses force only to contain alleged lawbreakers until a judicial forum can determine personal culpability. An action legitimately in the realm of national security law may be intolerant of any injury and, when hostile intent is perceived, may authorize a strike to prevent it from occurring. Law enforcement constructs presume the innocence of suspects and endure the losses that forbearance in the name of legal process occasionally imposes.

All things being equal, cyber strategists should default to the law enforcement modality. This makes practical sense, because many experts see cyber crime (as opposed to cyberwar) as the most serious and most common threat in the cyber domain.[20] "Crime," incidentally, could include acts at the behest of a nation-state, such as cyber espionage targeting a government or industry. As a general proposition, nondestructive computer methodologies employed for espionage may violate the domestic law of the victim nation-state but are not contrary to international law.[21]

In any event, "act of war" is a political phrase, not a legal term.[22] It might be said that the United Nations Charter was designed, in essence, to ban "war" from the lexicon of nations.[23] Article 2 (4) of the Charter demands that nations "refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state."[24] It sanctions only two exceptions to this prohibition on the use of force: (1) when the Security Council authorizes force, and (2) when a nation acts in self-defense. As to self-defense, Article 51 says

that nothing in the Charter shall "impair the inherent right of individual or collective self-defense if an armed attack occurs" against a UN member.[25] It is this self-defense provision that often confounds cyber strategists and their lawyers. Why?

The logic can be confusing. Specifically, Article 2 prohibits all threats and uses of "force," while Article 51 allows the use of force *only* in response to a certain kind of attacking force, specifically, an "armed attack." Retired Air Force colonel turned law professor Michael N. Schmitt notes that "all armed attacks are uses of force [within the meaning of Article 2], but not all uses of force qualify as armed attacks" that are a prerequisite to an *armed* response.[26] Thus, a nation may be the victim of cyber "force" of some sort being applied against it but cannot respond in kind because the force it suffered did not amount to an armed attack. However, a victim state may engage in a number of activities short of the use of force, including the unilateral severance of economic and diplomatic relations, civil lawsuits, and application to the UN Security Council for further action. In appropriate cases, pursuing criminal prosecution is an option.[27]

Of course, a cyber technique *can* qualify as an armed attack. Cyber methodologies may qualify as "arms" under certain circumstances,[28] and existing LOAC provisions provide ready analogies for construing their use as an "attack." Specifically, although cyber techniques may not involve kinetics, as a matter of law an attack may take place even without a weapon that uses them. *Protocol I* to the Geneva conventions defines *attacks* to mean "acts of violence against an adversary,"[29] which is properly interpreted to "extend to violent consequences of an attack which does not consist of the use of kinetic force."[30] The leading view, therefore, among legal experts focuses on the consequences and calls for an *effects-based* analysis of a particular cyber incident to determine whether or not it equates to an "armed attack" as understood by Article 51.[31]

Schmitt pioneered this approach and offers seven factors to consider in making the judgment as to whether a particular cyber event constitutes "force" at all: severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy, and responsibility.[32] It is beyond the scope of this article to detail the nuances of each of those factors,[33] but it is important to understand that in determining whether the cyber activity is severe enough to amount to the legal equivalent of an armed attack (as opposed to merely a use of some force), the consequences must extend to more than mere inconvenience; there must be at least temporary damage of

some kind.[34] Schmitt points out that the "essence of an 'armed' operation is the causation, or risk thereof, of death or injury to persons or damage to or destruction of property and other tangible objects."[35]

Cyber events that have violent effects are, therefore, typically the legal equivalent to armed attacks. To be clear, not all adverse cyber events qualify; accordingly, before responding in any way that constitutes a use of force—to include even actions that do not amount to an armed attack—the evidence must show that the effects of the triggering event amount to the equivalent of an armed attack. If they do not reach that level, the response must be limited to acts like those mentioned above which do not amount to a use of force. Dispassionately assessing the consequences of a cyber incident to determine their similarity to an armed attack can be difficult, as initial impressions of the effects can be wildly inflated.

Further convoluting the analysis is the fact that not all damaging cyber events that seemingly equate to an armed attack may be sufficiently egregious to authorize the use of any kinetic or cyber force in response. Although not involving cyber matters, an opinion of the UN–sanctioned International Court of Justice (ICJ) provides some insight. In *Nicaragua v. U.S.*, the ICJ seemed to indicate that an armed attack within the meaning of Article 51 did not arise in every case of an armed clash. Rather, the ICJ considered the "scale and effects" of the use of force to determine if it met the Article 51 requirement.[36]

As an illustration of inadequate levels of violence, the ICJ cited a "mere frontier incident."[37] Although the court did not elaborate on this example, the context implies that such an incident would involve some low level of violence. While apparently accepting (without using the words) the concept of an effects-based approach, the ICJ nevertheless held that "assistance to rebels in the form of the provision of weapons or logistical or other support" was insufficient provocation for an Article 51 response.[38] Such activities may be uses of force prohibited by Article 2 of the UN Charter but do not equate to armed attacks so as to permit self-defense (Art. 51) actions involving the use of force.

Because not every disturbance sourced in a cyber methodology amounts to an armed attack under international law, the Department of Defense (DoD) definition of "computer network attack" is not necessarily coterminous with what cyber strategists should consider as sufficient to trigger a response involving the use of force. Specifically, the DoD characterizes *attack* as actions "taken through the use of computer networks to disrupt,

deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves." Quite obviously, this definition takes no cognizance of "scale and effects" and would, therefore, encompass events that are the legal equivalent—in the cyber world—of the "mere frontier incidents" that the ICJ found did not permit an Article 51 response.

The principle of self-defense is also complicated by the issue of anticipatory or "preemptive" self-defense. This is important to cyber strategists as cyber weaponry can be employed rapidly and, once a cyber strike is underway, can be difficult to counter or contain. Nevertheless, many nations claim that bona fide self-defense actions can only be taken *after* an armed attack, not before.[39] However, the United States and some other countries insist that it permits the use of force before suffering actual injury; that is, taking a self-defense action that anticipates and deflects the blow or otherwise preempts an aggressor's ability to take the proverbial "first shot." So long as the response was proportional to the threat posed, the act is lawful.

Classic anticipatory self-defense theory requires evidence that a specific attack is imminent; that is, about to occur. However, American University law professor Kenneth Andersen argues that since at least 1980,

> [the United States] has taken the position that imminence can be shown by a pattern of activity and threat that show the intentions of actors. This can satisfy imminence whether or not those intentions are about to be acted upon. Even events taking place in the past can suffice if the risk is severe enough, and those events can include meeting, planning, and plotting. It is not necessarily or only about a threatened specific event, but about a group or a threat in some broader way. This is sometimes called "active self defense."[40]

This may be attractive to some cyber strategists who want a legal basis to take defensive actions that amount to a use of force against suspicious threats. However, disaggregating intent from capability could have unintended consequences. For example, it may behoove cyber strategists to avoid embracing a legal interpretation that would categorize the nondestructive insertion of a cyber capability into the computer system of another nation as either a use of force or an armed attack. The better view today would be that such activities—without an accompanying intent for imminent action—would not be uses of force, so long as the cyber capability lies dormant.

In interpreting self-defense under Article 51, cyber strategists should keep in mind that the UN Charter governs relations between nation-states, not individuals. The DoD general counsel opines that when "individuals carry

out malicious [cyber] acts for private purposes, the aggrieved state does not generally have the right to use force in self-defense."[41] To do so ordinarily requires some indicia of effective state control of the cyber actors to impute state responsibility.[42]

Nevertheless, if the aggrieved nation requests action from the state from whose territory the cyber attack was carried out and it becomes evident that the state is "unwilling or unable to prevent a recurrence," actions in self-defense are justified.[43] This is the rationale to which Harold Koh, legal advisor to the State Department, alluded when he spoke about self-defense in the context of "the willingness and ability of those nation-states to suppress the threat the target poses."[44] Of course, the problem of attribution stubbornly permeates every aspect of cyber operations; it is, indeed, the "single greatest challenge to the application of the law of armed conflict to cyber activity."[45] Essentially, however, this is a technical issue, not a legal one. Nonetheless, the identity of the attacker may well determine if a state of war exists.

A State of War?

Even the occurrence of a cyber event that equates to an armed attack warranting a lawful self-defense response does not automatically create a state of war (or armed conflict).[46] The presence—or absence—of a state of armed conflict carries significance, because during armed conflict the actions of belligerents are usually governed by LOAC, not the more-restrictive rules applicable to law enforcement situations. In determining the existence of a state of war, we look to traditional definitions, the clearest of which is offered by scholar Yoram Dinstein, who describes it as:

> [A] hostile interaction between two or more States, either in a technical or in a material sense. War in the technical sense is a formal status produced by a declaration of war. War in the material sense is generated by actual use of armed force, which must be comprehensive on the part of at least one party to the conflict.[47]

For cyber strategists, the words "States," "armed force," and "comprehensive" are key because they help distinguish the actions of criminals or cyber vandals from the persistent and comprehensive cyber attacks equating to armed force that increasingly appear to be only within the capability of nation-states. As a matter of legal interpretation, nation-states do not wage *war* against criminals; rather, they conduct law enforcement operations against them. As Schmitt notes, "Cyber violence of any intensity engaged

in by isolated individuals or by unorganized mobs, even if directed against a government," does not create an armed conflict within the meaning of the Geneva conventions.[48]

That said, certain nonstate adversaries can make themselves subject to much the same LOAC regime as a conventional state (albeit without some of the privileges to which a nation-state combatant is entitled). Jamie Williamson, legal counsel to the International Committee of the Red Cross (ICRC), acknowledges that nonstate actors organized into armed groups can constitute "the armed forces of a nonstate party."[49] In accord is Koh's declaration that "as a matter of international law, the United States is in an armed conflict with al-Qaeda," which he characterizes as an "organized terrorist enemy."[50] And this same reasoning applies to the cyber setting. Schmitt observes that "only significantly destructive [cyber] attacks taking place over some period of time and conducted by a group that is well-organized" is sufficient to constitute an internationally recognized armed conflict.[51]

When a state of armed conflict exists, the "fundamental targeting issues are no different in cyber operations as compared to those applicable to kinetic targeting."[52] Koh summarizes the most important of these issues:

> First, the principle of distinction, which requires that attacks be limited to military objectives and that civilians or civilian objects shall not be the object of the attack; and Second, the principle of proportionality, which prohibits attacks that may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, that would be excessive in relation to the concrete and direct military advantage anticipated.[53]

Regarding the targeting of civilians and civilian objects, it is also true that only weaponry (cyber or kinetic) capable of discrimination (i.e., directed against legitimate targets) can be used.[54] However, cyber strategists should know that legitimate targets can include civilian objects—especially those having cyber aspects—that have dual military and civilian uses.[55] So long as the principal of proportionality is observed, these normally can be targeted lawfully if they meet the definition of a military objective.[56]

In this area particularly, cyber strategists need to distinguish prudent targeting from legal mandates. In his confirmation hearings, General Alexander said that it "is difficult for me to conceive of an instance where it would be appropriate to attack a bank or a financial institution, unless perhaps it was being used solely to support enemy military operations."[57] However sensible that may be from a policy perspective, cyber strategists should

understand that no LOAC rule requires a target that otherwise qualifies as a military objective to be used *solely* to support military operations—it can have *dual* uses.

Of course, there is no such thing as a "dual use" civilian, but civilians can be targeted consistent with the principle of distinction under certain limited circumstances. Williamson of the ICRC accepts that international law permits the targeting of civilians for such time as they "directly participate in hostilities." If they are members of an organized armed group of nonstate actors, the period of vulnerability may be extended to parallel that of the uniformed military of nation-states; that is, they would be subject to attack virtually at any time or place during an ongoing conflict. However, he advises that the ICRC "takes a 'functional'—not membership—approach." So defined, the nonstate "armed force" consists "only of individuals whose constant function is to take a direct part in hostilities, or, in other words, individuals who have a continuous combat function."[58]

In determining what amounts to a "continuous combat function" in the cyber context, consider the ICRC illustrations. Its examples of "direct participation" by civilians in hostilities include such cyber activities as "[i]nterfering electronically with military computer networks (computer network attacks) and transmitting tactical targeting intelligence for a specific attack."[59] Accordingly, a civilian can be targeted when performing those acts, and one who continuously engages in such conduct can be said to have a continuous combat function, making that person susceptible to attack for as long as that status persists. To anticipate what other cyber activities one might reasonably determine to constitute direct involvement in hostilities, it may help for cyber strategists to consider what activities of the enemy they would consider so intrinsic to a particular cyber process that they would need to target as a matter of military necessity.

As Koh's remarks suggest, LOAC tolerates "incidental" losses of civilians and civilian objects so long as they are "not excessive in relation to the concrete and direct military advantage anticipated." In determining the incidental losses, cyber strategists are required to consider those that may be reasonably foreseeable to be directly caused by the attack. Assessing second- and third-order "reverberating" effects may be a wise policy consideration,[60] but it does not appear LOAC currently requires such further analysis. Another hurdle for cyber strategists may be the difficulty in predicting the effect of a given cyber methodology. Absent a suitable cyber modeling capability that estimates civilian losses, it is unclear how a decision

maker fulfills the legal requirement to weigh those effects against the military advantage sought.

LOAC does require that targeteers "do everything feasible" to ensure the target is a proper military objective.[61] How sure must a cyber strategist be? International courts have used the "reasonable commander" standard; that is, whether the decision is one that a "reasonably well informed person in the circumstances of the actual perpetrator, making reasonable use of the information available to him or her" would have concluded the target met the legal standards.[62] As to degree of certainty, Schmitt offers a "clear and compelling standard" which is "higher than the preponderance of evidence . . . standard used in certain civil and administrative proceedings and lower than criminal law's 'beyond a reasonable doubt' " criterion.[63]

Parenthetically, this discussion of civilians has other implications for cyber strategists; that is, who may conduct cyberwar? Generally, only bona fide members of the armed forces can wage war with the protection of the "combatant privilege." This means so long as LOAC is otherwise observed, military personnel are legally permitted to engage in killing and destruction in war without fear of prosecution for doing so. Thus, conducting cyber activities which have the lethality and destructiveness of traditional kinetic weaponry should be reserved to uniformed members of the military. As Richard Clark states in *Cyberwar*, "It will have to be . . . military personnel [who] enter the keystrokes to take down enemy systems."[64]

In a *Washington Post* op-ed, LOAC expert (and retired Marine Corps judge advocate) Gary Solis takes a harsh view of civilians operating lethal systems. Calling CIA drone pilots "America's own unlawful combatants," he accuses them of "employing armed force contrary to the laws and customs of war" and "violating the requirement of distinction, a core concept of armed conflict."[65] Although Solis is correct in saying that if captured, CIA civilian employees (and/or CIA contractors) are not entitled to prisoner of war status and that they could be legally tried a under the capturing state's domestic law, is his insinuation of war crimes overstated?

A 1999 DoD publication provides some insight. Specifically, in discussing "retaining the requirement that combatant information operations during international armed conflicts be conducted only by members of the armed forces," the DoD general counsel opined that if cyber operations (amounting to a use of armed force) are "conducted by unauthorized persons, their government may be in violation of the law of war, depending on the circumstances, and the individuals concerned are at least theoretically

subject to criminal prosecution either by the enemy or by an international war crimes tribunal."[66]

Cybering and the Citizenry

The nature of the cyber domain is such that it necessarily involves consideration of the domestic environment and its citizenry. Somewhat paradoxically, given the above discussion about the role of civilians in cyberwar, concerns also arise about the appropriate role of the armed forces in cyber operations, especially in situations short of armed conflict.

The vast majority of cyberspace usage involves the lawful activities of the public. As the U.S. armed forces are generally outwardly focused towards external threats, friction with the citizenry has been largely avoided. Unfortunately, the military intelligence apparatus has occasionally been improperly turned inward "to collect personal information about Americans who posed no real threat to national security."[67] The technical potential to do so today is very great. For example, every day the DoD—via the National Security Agency (NSA)—"intercept[s] and store[s] 1.7 billion e-mails, phone calls and other types of communications."[68] Moreover, it is continually seeking new cyber systems to collect even greater quantities of information more broadly and effectively.[69] Of course, these military intelligence capabilities were designed to address external threats, but they are being exploited to address domestic security.

Regrettably, incidents of impropriety still occur. In the aftermath of 9/11, the NSA was "secretly given authority to spy on Americans as part of the war on terrorism."[70] Specifically, the NSA was allowed to eavesdrop on phone calls, monitor e-mails, and track Internet activity without getting a warrant from the special courts established by the Foreign Intelligence Surveillance Act (FISA). The Justice Department vigorously defended what it described as a "terrorist surveillance program" by insisting that bypassing FISA procedures was legal and incident to the president's authority as commander in chief.[71] The courts found otherwise, and in late December 2010 the government was ordered to pay $2.5 million in attorney fees and damages for the NSA's illegal activity.[72]

Other unsettling incidents include reports of the unexplained military monitoring of Planned Parenthood and other organizations.[73] Media stories also show the military having "burrowed into the mushrooming cyber world of blogs" to post content in an attempt to "influence public opinion

about U.S. operations in Iraq and Afghanistan."[74] More recently, journalist Walter Pincus reports the military wanting to expand its intelligence role in cyberspace to counter what is called "the use of the Internet by extremists."[75] ADM James A. Winfield, commander of US Northern Command, says that although his command's role is to defend its networks, he has a "very ambitious staff, and they would like nothing more than to own all of the cyber response inside North America."[76]

Because it "possesses extraordinary technical expertise and experience, unmatched in the government, in exploring and exploiting computer and telecommunication systems," powerful imperatives are pushing further NSA involvement in domestic cyber activities.[77] In a major new development, a cyber security memorandum of agreement was executed between the DoD and the Department of Homeland Security (DHS) in October 2010.[78] For the first time, the DoD is becoming directly involved in protecting domestic civilian cyber infrastructure. To do so, an NSA "cyber-support element will move into Homeland Security's Cybersecurity and Communications Integration Center." Although DHS personnel are supposed to ensure privacy and the protection of civil liberties, Marc Rotenberg of the Electronic Privacy Information Center says he does not think "DHS can oversee the Defense Department."[79]

With powerful cyber systems like Einstein 3 coming online that call for a major NSA role, thoughtful experts like Jack Goldsmith of the Harvard Law School offer a roadmap for proceeding consonant with civil liberties. Among other things, he would require the NSA to obtain "independent approval . . . from the FISA court or a FISA-type court" prior to employing advanced cyber security measures domestically.[80] Legislation such as the Protecting Cyberspace as a National Asset Act now pending also includes safeguards intended to protect privacy and civil liberties.[81]

Nevertheless, cyber strategists may want to encourage the development of fully civilian domestic surveillance cyber systems and, concomitantly, discourage involvement of the armed forces in any cyber operations that might seem to conflict with the sensibilities and mores of the American people, even if technically legal. The armed forces are the most authoritarian, least democratic, and most powerful institution in American society. The restraint intrinsic to a domestic law enforcement mind-set is not its natural state; its purpose, as the Supreme Court puts it, is to wage war.[82] And as this article and other sources suggest, relatively few cyber incidents, domestic or global, meet that legal standard.[83] If nothing else, the fact

that the armed forces unapologetically restrict the rights and privileges of their own members[84] should militate toward avoiding their use in civilian settings where the public properly expects those rights and privileges to flourish.

Cyber strategists need to be especially conscious of emerging public attitudes. As experts question whether the threat of terrorism[85] and even the threat of cyberwar are overstated,[86] Americans may be becoming uncomfortable with what Fareed Zakaria describes as the "national-security state [that] now touches every aspect of American life, even when seemingly unrelated to terrorism."[87] The recent furor over full-body scans at airports, along with a generalized distrust of government,[88] reflects what could be burgeoning public discontent with intrusive government activity (some of which may already be percolating with respect to military cyber activities).[89] In short, cyber strategists must be extremely sensitive to involving the DoD in domestic cyber activities that might align such animosity with the armed forces, as this could undermine the public support and esteem they need to sustain and prevail on tomorrow's battlespaces.

Concluding Observations

Cyber activities do present a number of legal challenges for cyber strategists, but many problems masquerading as "legal" issues are really undecided policy issues with a number of legal alternatives. Cyber strategists rightly carry a heavy element of complicated and difficult policymaking, because cyber issues are so entwined with the lawful activities of citizens and the legitimate needs of commerce.

Solid legal advice in cyber matters is imperative, and the Pentagon is moving to improve its resources to provide it.[90] As one expert put it, in today's world, law is a "center of gravity" because "our enemies carefully attack our military plans as illegal and immoral and our execution of those plans as contrary to the law of war."[91] Closer to home, cyber strategists may wish to consider the admonition of Michael Riesman and Chris Antoniou in their 1994 book, *The Laws of War*, that for democracies like the United States, "even a limited armed conflict requires a substantial base of public support." That support "can erode or even reverse itself rapidly, no matter how worthy the political objective, if people *believe* that the war is being conducted in an unfair, inhumane, or iniquitous way" (emphasis added).[92]

In cyberwar, like any other conflict, victory depends much on what people believe. Cyber strategists would be well served to ensure that what they do in the coming years not only meets the challenges in cyberspace, but also fulfills the American people's expectations of all their warriors, regardless of the domain in which they operate. SSQ

Notes

1. See, for example, John Sutter, "Is Wikileaks engaged in 'Cyberwar'?" *CNN*, 9 December 2010, http://articles.cnn.com/2010-12-09/tech/wikileaks.cyber.attacks_1_cyber-war-cyber-weapons-cyber-attacks?_s=PM:TECH.

2. For a discussion of the Estonia and Georgia incidents, see Richard A. Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: HarperCollins, 2010), 11–21.

3. Norman Friedman, "Virus Season," *Proceedings* 136, no. 11 (November 2010): 88.

4. For purposes of this article, *cyberwar* may be defined as conflict waged by means of *cyber operations*. The latter are, in turn, defined by the DoD to be "employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace." The DoD defines *cyberspace* as "global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." Joint Publication 1-02, *DoD Dictionary of Military and Associated Terms*, as amended through 30 September 2010, 118, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

5. LTG Keith B. Alexander, USA, quoted in Thom Shanker, "Cyberwar Nominee Sees Gaps in Law," *New York Times,* 14 April 2010, http://www.nytimes.com/2010/04/15/world/15military.html.

6. Jeffrey F. Addicott, "Cyberterrorism: Legal Policy Issues," in *Legal Issues in the Struggle against Terrorism*, eds. John N. Moore and Robert F. Turner (Durham, NC: Carolina Academic Press, 2010), 550.

7. This article considers LOAC to encompass jus ad bello (the international law which rationalizes recourse to armed conflict) and jus in bello (the international law which governs actions during armed conflict). For a discussion of jus ad bello and jus in bello in the cyber context, see, CDR Todd C. Huntley, JAGC, USN, "Controlling the Use of Force in Cyberspace: The Application of the Law of Armed Conflict During a Time of Fundamental Change in the Nature of Warfare," *Naval Law Review* 60 (2010): 1–40, http://www.jag.navy.mil/documents/navylawreview/NLRVolume60.pdf.

8. Strategist Carl von Clausewitz wrote: "The great uncertainty of all data in war is a peculiar difficulty, because all action must, to a certain extent, be planned in a mere twilight, which in addition not infrequently—like the effect of a fog or moonshine—gives to things exaggerated dimensions and unnatural appearance." Clausewitz, *On War*, bk. 2, chap. 2, par. 24.

9. See "Time for a Treaty" (editorial), *Defense News*, 18 October 2010, 36, http://www.defensenews.com/story.php?i=4921341.

10. Bruce Schneier, "It will soon be too late to stop the cyberwars," *Financial Times*, 2 December 2010, http://www.ft.com/cms/s/0/f863fb4c-fe53-11df-abac-00144feab49a.html#axzz19cNCeszp.

11. See John B. Alexander, "Optional Lethality: Evolving Attitudes towards Nonlethal Weaponry," *Harvard International Review*, 7 May 2006, http://hir.harvard.edu/the-future-of-war/optional-lethality.

12. Charles Krauthammer, "The Irrelevance of START," *Washington Post*, 26 November 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/11/25/AR2010112502232.html.

13. William J. Lynn, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* 89, no. 5 (September/October 2010), http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain.

14. See Richard W. Aldrich, "Information Warfare & the Protection of Critical Infrastructure," in *National Security Law*, 2d ed., eds. John N. Moore and Robert F. Turner (Durham, NC: Carolina Academic Press, 2005), 1243–44.

15. Tom Gjelten, "Shadow Wars: Debating Cyber 'Disarmament'," *World Affairs*, November/December 2010, http://www.worldaffairsjournal.org/articles/2010-NovDec/full-Gjelten-ND-2010.html.

16. Ibid.

17. Ibid. In 1999 the DoD Office of General Counsel concluded that "there seems to be no particularly good reason for the United States to support negotiations for new treaty obligations in most areas of international law that are directly relevant to information operations." Office of General Counsel, *An Assessment of International Legal Issues in Information Operations*, 2nd ed. (Washington: DoD, November 1999), 49, http://www.cs.georgetown.edu/~denning/infosec/DOD-IO-legal.doc [hereinafter *GC Memo*].

18. See Anna Mulrine, "When is a Cyberattack an Act of War?" *Christian Science Monitor*, 18 October 2010, 20, http://www.csmonitor.com/USA/Military/2010/1005/Pentagon-The-global-cyberwar-is-just-beginning.

19. Thomas Wingfield sees a third legal regime as applicable to cyber operations: intelligence collection law. Wingfield, in *Cyberpower and National Security*, ed. Franklin D. Kramer et al. (Washington: NDU Press, 2009), 541.

20. Elinor Mills, "Demilitarizing Cyberspace (Q&A)," *Tech Reviews* blog, December 2010, http://tech-reviews.findtechnews.net/demilitarizing-cybersecurity-qa/.

21. Walter Gary Sharp Sr., *Cyberspace and the Use of Force* (San Antonio, TX: Aegis Research Corp., 1999), 123–32.

22. See *GC Memo*, 11. Act of war is an "obsolete concept not mentioned in the UN Charter and seldom heard in modern diplomatic discourse."

23. *Charter of the United Nations and Statute of the International Court of Justice* (San Francisco: United Nations, 1945), http://treaties.un.org/doc/Publication/CTC/uncharter.pdf.

24. Ibid., 3.

25. Ibid., 10.

26. Michael N. Schmitt, "Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflict," in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (Washington: National Academies Press, 2010), 163, http://books.nap.edu/openbook.php?record_id=12997&page=R1.

27. For example, see Jeffrey F. Addicott, *Terrorism Law: Materials, Cases, Comments* (Tucson, AZ: Judges and Lawyers Publishing Co., 2011), 311–12.

28. Wg Cdr Duncan Blake, RAAF, and Lt Col Joseph S. Imburgia, USAF, " 'Bloodless weapons'? The need to conduct legal reviews of certain capabilities and the implications of defining them as 'weapons'," *Air Force Law Review*, 14 December 2010, 181–83.

29. *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I),* 8 June 1977, Art. 49.1, http://www.icrc.org/ihl.nsf/7c4d08d9b287a42141256739003e636b/f6c8b9fee14a77fdc125641e0052b079. Although the United States is not a party to *Protocol I*, it accepts that most of it comprises customary international law which binds all nations.

30. William Boothby, *Weapons and the Law of Armed Conflict* (Oxford, UK: Oxford Scholarship Online, 2009), 238.

31. See David E. Graham, "Cyber Threats and the Law of War," *Journal of National Security Law* 4, no. 1 (2010): 91, for a discussion of the "instrument-based approach" and the "strict liability" approach as competing analyses.

32. Schmitt, "Cyber Operations in International Law," 155–56.

33. For a discussion of the Schmitt criteria, see Wingfield, "International Law and Information Operations,"527–31.

34. Boothby, *Weapons and the Law of Armed Conflict*.

35. Schmitt, "Cyber Operations in International Law."

36. *Military and Paramilitary Activities in and against Nicaragua* (*Nicar. v. U.S.*), 1986 I.C.J. 14 (June 27), para. 195.

37. Ibid.

38. Ibid.

39. Michael Byers, *War Law: Understanding International Law and Armed Conflict* (New York: Grove Press, 2005), 72–81.

40. Kenneth Anderson on *Baumann v. Wittes*, *Lawfare* blog, 1 December 2010, http://www.lawfareblog.com/2010/12/kenneth-anderson-on-baumann-v-wittes/.

41. *GC Memo*, 20.

42. Schmitt, "Cyber Operations in International Law," 157.

43. *GC Memo*, 20.

44. Harold Koh, "The Obama Administration and International Law," speech, American Society of International Law, 25 March 2010, http://www.state.gov/s/l/releases/remarks/139119.htm.

45. Huntley, "Controlling the Use of Force in Cyberspace," 34.

46. In this context, "war" and "armed conflict" are interchangeable.

47. Yoram Dinstein, *War, Aggression and Self-Defence*, 4th ed. (Cambridge, UK: Cambridge University Press, 2005), 15.

48. Schmitt, "Cyber Operations in International Law," 175.

49. Jamie A. Williamson, "Challenges of Twenty-First-Century Conflicts: A Look at Direct Participation in Hostilities," *Duke Journal of Comparative & International Law* 20, no. 3 (Spring 2010): 464, http://www.law.duke.edu/journals/djcil/.

50. Koh, "Obama Administration and International Law."

51. Schmitt, "Cyber Operations in International Law," 176.

52. *Air Force Operations & the Law* (Maxwell AFB, AL: USAF Judge Advocate General's School, 2009), 99.

53. Koh, "Obama Administration and International Law."

54. See Burris Carnahan, "Weapons," in *Crimes of War: What the Public Should Know*, eds. Roy Gutman and David Rieff (New York: W. W. Norton, 1999), 380, http://www.crimesofwar.org/thebook/weapons.html.

55. See James P. Terry, "The Lawfulness of Attacking Computer Networks in Armed Conflict and in Self Defense During Periods Short of Armed Conflict: What Are the Targeting Constraints?" *Military Law Review* 69 (September 2001): 70.

56. *Military objectives* are defined as "those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage." *Protocol I,* Art. 49.1.

57. Alexander quoted in Shanker, "Cyberwar Nominee Sees Gaps in Law."

58. Williamson, "Challenges of Twenty-First-Century Conflicts."

59. "Direct Participation in Hostilities: Questions and Answers," International Committee of the Red Cross, 2 June 2009, http://www.icrc.org/eng/resources/documents/faq/direct-participation-ihl-faq-020609.htm.

60. See CDR J. W. Crawford, "The Law of Noncombatant Immunity and the Targeting of National Electrical Power Systems," *Fletcher Forum of World Affairs*, Summer/Fall 1997, 101.

61. *Protocol I*, Art. 57.2(a)(i).

62. See Laurie Blank and Amos Guiora, "Teaching an Old Dog New Tricks: Operationalizing the Law of Armed Conflict in New Warfare," *Harvard National Security Journal* 1 (13 May 2010): 56–57, citing *Prosecutor v. Stanislav Galic*, http://www.harvardnsj.com/wp-content/uploads/2010/05/Vol.-1_Blank-Guiora_Final.pdf.

63. Schmitt, "Cyber Operations in International Law," 168.

64. Clarke and Knake, *Cyber War*, 40.

65. Gary Solis, "CIA drone attacks produce America's own unlawful combatants," *Washington Post*, 12 March 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/03/11/AR2010031103653.html.

66. *GC Memo*, 7.

67. Stephen Dycus et al., "The Military's Role in Homeland Security and Disaster Relief," in *National Security Law*, 4th ed. (New York: Aspen Publishers, 2007), 960.

68. Dana Priest and William Arkin, "A Hidden World, Growing beyond Control," *Washington Post*, 19 July 2010, http://projects.washingtonpost.com/top-secret-america/articles/a-hidden-world-growing-beyond-control/?referrer=emaillink.

69. See Steve Lohr, "Computers That See You and Watch Over You," *New York Times*, 1 January 2011, 1, discussing the Defense Advanced Research Projects Agency's award of a grant for a research program called the Mind's Eye, which seeks "machines that can recognize, analyze and communicate what they see," http://www.nytimes.com/2011/01/02/science/02see.html?hp; and Siobhan Gorman, "U.S. Plans Cyber Shield for Utilities, Companies," *Wall Street Journal*, 8 July 2010, discussing an "expansive" NSA program "dubbed 'Perfect Citizen'," http://online.wsj.com/article/SB10001424052748704545004575352983850463108.html.

70. DoD News Release, "Joint Statement by Secretary Gates and Secretary Napolitano on Enhancing Coordination to Secure America's Cyber Networks," 13 October 2010, http://www.defense.gov/releases/release.aspx?releaseid=13965.

71. Department of Justice Public Affairs, "The NSA Program to Detect and Prevent Terrorist Attacks: Myth v. Reality," 27 January 2006, http://www.justice.gov/opa/documents/nsa_myth_v_reality.pdf.

72. Paul Elias, "Judge Orders Feds to Pay $2.5 million in Wiretapping Case," *Washington Post*, 21 December 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/12/21/AR2010122105307.html.

73. Kim Zetter, "Military Monitored Planned Parenthood, Supremacists," *Wired* magazine, 25 February 2010, http://www.wired.com/threatlevel/2010/02/military-spied-on-planned-parenthood/.

74. Jason Sherman, "CENTCOM Eyes Blogs to Shape Opinion," *Military.com*, 3 March 2006, http://www.military.com/features/0,15240,89811,00.html.

75. Walter Pincus, "Military Expands Intelligence Role," *Washington Post*, 8 June 2010, A-15, http://www.washingtonpost.com/wp-dyn/content/article/2010/06/07/AR2010060704696.html.

76. Quoted in Mark V. Schanz, "Air Sovereignty Never Sleeps," *Air Force Magazine*, December 2010, 56, http://www.airforce-magazine.com/MagazineArchive/Documents/2010/December%202010/1210sovereignty.pdf.

77. Jack Goldsmith, *The Cyberthreat, Government Network Operations, and the Fourth Amendment* (Washington: Brookings Institution, 8 December 2010), 15, http://www.brookings.edu

/~/media/Files/rc/papers/2010/1208_4th_amendment_goldsmith/1208_4th_amendment_goldsmith.pdf.

78. DoD News Release, "Joint Statement by Secretary Gates and Secretary Napolitano."

79. William Matthews, "DoD to Protect Some Civilian Infrastructure," *Defense News*, 18 October 2010, 6.

80. Goldsmith, *Cyberthreat,* 14.

81. See Senate press release, "Lieberman, Collins, Carper Unveil Major Cybersecurity Bill to Modernize, Strengthen, and Coordinate Cyber Defenses," 10 June 2010, for a link to the bill, http://hsgac.senate.gov/public/index.cfm?FuseAction=Press.MajorityNews&ContentRecord_id=227d9e1e-5056-8059-765f-2239d301fb7f.

82. The "primary business of armies and navies [is] to fight or be ready to fight wars should the occasion arise." *United States ex rel. Toth v. Quarles*, 350 U.S. 11 (1955).

83. See Gary McGraw and Ivan Arce, "Software [In]security: Cyber Warmongering and Influence Peddling," *informIT.com*, 24 November 2010, http://www.informit.com/articles/article.aspx?p=1662328#.

84. "The rights of men in the armed forces must perforce be conditioned to meet certain overriding demands of discipline and duty." *Burns v. Wilson*, 1953, 346 U.S. 137 (1953). "The essence of military service is the subordination of the desires and interests of the individual to the needs of the service." *Goldman v. Weinberger*, 475 U.S. 503 (1986).

85. Risk-management experts John Mueller and Mark G. Stewart conclude from a survey of many studies that the risk of terrorism is "hardly existential" and is, in fact, "so low that spending further to reduce its likelihood or consequences is scarcely justified." See Mueller and Stewart, "Hardly Existential: Thinking Rationally about Terrorism," *Foreign Affairs.com*, 2 April 2010, http://www.foreignaffairs.com/articles/66186/john-mueller-and-mark-g-stewart/hardly-existential.

86. See Seymour M. Hersh, "The Online Threat," *New Yorker*, 1 November 2010, http://www.newyorker.com/reporting/2010/11/01/101101fa_fact_hersh.

87. Fareed Zakaria, "What America Has Lost; It's Clear We Overreacted to 9/11," *Newsweek*, 13 September 2010, 18, http://www.newsweek.com/2010/09/04/zakaria-why-america-overreacted-to-9-11.html.

88. See Mark Silva, "Few trust the government, poll finds," *Los Angeles Times*, 19 April 2010, http://articles.latimes.com/2010/apr/19/nation/la-na-distrust19-2010apr19.

89. See Hersh, "Online Threat."

90. The new DoD *Law of War Manual* is expected to have a "17-page chapter on information and cyberspace operations." See W. Hays Parks, "National Security Law in Practice: The Department of Defense *Law of War Manual*," speech, 18 November 2010, http://www.abanet.org/natsecurity/hays_parks_speech11082010.pdf.

91. William George Eckhardt, "Lawyering for Uncle Sam When He Draws His Sword," *Chicago Journal of International Law 4, no. 2 (Fall 2003): 431.*

92. W. Michael Reisman and Chris T. Antoniou, eds., *The Laws of War* (New York: Vintage, 1994), xxiv.

World Gone Cyber MAD

How "Mutually Assured Debilitation" Is the Best Hope for Cyber Deterrence

Matthew D. Crosston

In the unseen reaches of cyberspace, our enemies are quietly taking the postmodern form of warfare we witnessed on September 11 to a new level: they are no longer just transnational—they are non-national, hiding and attacking in a world where there are no borders. They are no longer just stateless—they are place-less. And they are no longer virtually invisible—they are, well, virtual.

—Alan W. Dowd, *Fraser Forum* (2008)

Many cyber experts say the United States is woefully ill prepared for a sophisticated cyber attack and that each passing day brings it one step closer to a potential virtual Armageddon. While the problems hindering the development of an effective and comprehensive cyber deterrence policy are clear (threat measurement, attribution, information-sharing, legal codex development, and poor infrastructure, to name several), this article focuses on one aspect of the debate that heretofore has been relatively ignored: that the futility of governmental innovation in terms of defensive efficacy is a relatively constant and shared weakness across all modern great powers, whether the United States, China, Russia, or others. In other words, every state that is concerned about the cyber realm from a global security perspective is equally deficient and vulnerable to offensive attack; therefore, defensive cyber systems are likely to remain relatively impotent across the board.

The United States tends to view this problem as if it has a unique burden to bear. While smaller states that do not envision a global role for themselves fear a massive cyber attack far less than the United States, this is not necessarily true of the aforementioned states and others that wish to

---

Dr. Matthew Crosston is director of the International Security and Intelligence Studies Program and chair of political science at Bellevue University. A graduate of Colgate and Brown, he has specialized in issues of national security, especially in regards to democracy promotion, terrorism prevention, and new concepts in future conflict. He also works to promote interaction abroad between intelligence agencies that share common interests but are without channels of connectivity.

be important global players. As a consequence, the goal for major powers should not be the futile hope of developing a perfect defensive system of cyber deterrence, but rather the ability to instill deterrence based on a mutually shared fear of an offensive threat. The United States is better positioned by shifting to an open, transparent policy that seeks to infer deterrence from the efficacy of its offensive cyber capabilities. This strategy has greater probability of staying ahead of rival deterrence systems and establishing the perception amongst rivals that the United States would indeed have effective second-strike capabilities if attacked. True, the goal for any major power would be to achieve dominance over such capabilities (such is the way with great powers), but this would also result in the problem of cyber security morphing into a zero-sum game where one state's dominance increases the insecurity of all others. For this reason it is logically more stable and potentially peaceful to have a system of deterrence that is structured mutually across major powers, giving no one state the ability to disrupt cyber equilibrium.

If adopted, this policy shift could hold the same potential that made nuclear mutually assured destruction (MAD) so effective for so long without being physically challenged through global war. Nuclear deterrence initially built off of the expected second-strike capability of being able to survive an initial strike long enough to launch an equally devastating counterstrike. But over time—as the great nuclear powers continued to build up huge arsenals—the de facto effectiveness of nuclear deterrence was not so much based on the likelihood of a second-strike capability but rather on the acceptance by all players that engaging in the nuclear game would inevitably bring devastation to all. A logic of deterrence emerged from an admission of being defenseless.

Perhaps it could be so with this new cyber "MAD"—in an open and transparent offensive system of cyber threat, each major player in the global system would come to fear debilitation equally and therefore would not risk being the first-strike initiator. By capitalizing on this shared vulnerability to attack and propagandizing the open buildup of offensive capabilities, there would arguably be a greater system of cyber deterrence keeping the virtual commons safe. Though it may seem oxymoronic, the more effective defense in this new world of virtual danger is a daunting cyber-lethal offensive capability; not so much to actually use it, but rather to instill the fear of it being used. And while the anarchic chaos and freedom of the Internet will always be a haven for nonstate actors looking to inflict

damage upon state systems, an open and transparent cyber-MAD policy would systematically give major powers the second-strike capability to potentially influence and deter these nonstate actors as well. Presently, defensive cyber deterrence systems basically give these actors free reign.

Interestingly, some states are clearly already adhering to this strategy, at least in the informal sense if not in explicit policy position—China's fervent support of "honkers" and the Russian Federation's frequent reliance upon "patriotic hackers" come to mind most readily. The United States certainly has the technological capability to equal Chinese and Russian virtual lethality. The formal lack of an open policy arguably indicates hesitancy on the part of the United States to develop a "weaponized virtual commons." Rather than an indication of infeasibility, this reluctance seems to be a nod to intelligence considerations, meaning the United States is arguably more satisfied developing its offensive capabilities in secret as part of more-covert operations than as a piece of overt policy. This article argues the emphasis on covert offensive capability rather than overt is an error that compromises the effectiveness of American cyber security.

The Need for a New Doctrine, New Questions, and New Answers

Institutional inertia and doctrinal rigidity are often major obstacles blocking policy reform and may even hinder the emergence of new policy ideas. However, in the cyber realm these blockades are not nearly as entrenched as other security issues/principles. For the past 10 years cyber security has become an increasingly important area of national interest; however, the cyber security context is a completely new era of thinking and dangers. It was not until late in the second term of Pres. George W. Bush that more definitive efforts were made across agencies to explicitly develop something akin to a national cyber doctrine (most vivid in this governmental newness was the 2009 creation of US Cyber Command). As analyst Mark Young recently argued,

> A national cyber doctrine is necessary. It is the link between strategy and the execution of the missions of the national security sector. Doctrine may traditionally be a military notion, but agencies are acknowledging the wisdom of establishing guiding principles. A national cyber doctrine can be a vehicle used to define the roles of departments and agencies for the entire U.S. government. In contrast to a presidential executive order or a National Security Council directive, a doctrine is developed in an openly collaborative fashion.[1]

This evidence attests to the absence of an open, overt, well-defined policy guiding long-term American interests over the issue of cyber security. Young rightly acknowledges that an explicit and well-defined cyber policy is essential to developing a comprehensive and effective cyber security system, largely because of the intense complexity inherent to cyber attacks and cyber deterrence. He continues,

> The nature of network attacks makes a well reviewed cyber doctrine particularly important, since national security leaders will have little time to consult with the National Security Council or the Commander in Chief when faced with an attack that could devastate the national economy, corrupt the flow of commerce, or disrupt military supply chains. Due to technical challenges, counterstrikes remain a time-consuming proposition. Disruption of a cyber attack is more easily achieved but may not be accomplished in time to protect critical data or national security systems.[2]

The main concern addressed by this article is that the debate to create a unified, explicit, and truly national cyber doctrine does not openly acknowledge the most basic axiom of the cyber realm: offense will always trump defense which, therefore, will not include all potential options and strategies.

To wit, the language cyber analysts and specialists use is inherently defensive—it is always about the problematic nature of counterstrikes, the technical challenges to disrupt an attack in progress, and lamenting the offensive advantage adversaries have over defensive specialists. These laments are real, but they inexplicably fail to lead the United States to the one potentially effective elephant sitting in the room that remains ignored or consistently talked around: the national cyber doctrine of the United States should not be based on defensive measures that are always going to hopelessly lag behind offensive measures, but rather on offensive capabilities that would give the explicit perception to potential adversaries that any aggressive maneuver will trigger debilitating retaliatory attacks more severe than any initial transgression—a true cyber-MAD policy, initially enshrining second-strike capability and, one would hope, institutionalizing the deterring admission of first-strike futility.

Some excellent work is already being done on the types of questions that need to be asked when considering cyber security options. While most of these questions presently address cyber deterrence from a purely defensive stance, the more important ones are still relevant for a cyber-MAD policy:

- Should the target reveal the cyber attack?

- When should attribution be announced?
- Should cyber retaliation be obvious?
- Is retaliation better late than never?
- Can there be confrontation without retaliation?[3]

All of these questions are incredibly important but have decidedly different answers, depending on what type of cyber-security system is being built. A purely defensive system rooted in intelligence secrecy produces ineffective answers that leave gaps in the national security infrastructure. Answers provided by an open, transparent, and offensive cyber-MAD policy would be aggressive and explicit enough to close these gaps by capitalizing on the logic and efficacy of nuclear deterrence. Openness and transparency render the "dilemma" of revealing targets and attribution problems moot, while a focus on offensive capability not only gives stronger teeth to retaliation but also creates the possibility of effective confrontation without retaliation and, ultimately, the avoidance of engagement outright. This was arguably the true legacy of peace left by nuclear deterrence. Could a cyber-MAD policy not produce the same hope?

One counterargument would answer no to that question: it is still impractical and unrealistic to think a cyber-MAD system can be effectively developed. There are simply too many problems in developing and guaranteeing that "mutually assured debilitation" can be achieved and, even if achieved, guaranteeing it can bring about the necessary threat deterrent to prevent or limit cyber attacks. In this case scholarship must be careful not to become purely academic and simply policy curmudgeons—stating that the cyber realm is a hopelessly offensive arena where deterrence based on defensive techniques cannot be effective, while also stating that a cyber deterrence system based on offensive technologies is equally impractical and ineffective. In other words, there is a tendency to declare that defense does not work *and* offense does not work simultaneously. This creates a scholarly and policy dead end, hopelessly charging intellectual windmills and getting nowhere.

Russian Rumors

The near virtual shutdown of Estonia in 2007 coincided with the Estonian government's decision to move a Soviet-era war memorial. In essence, the entire virtual framework within Estonia was inundated and overwhelmed

with "junk" for a period of three weeks. This essentially compromised if not temporarily crippled the Estonian communications network, as newspapers, mobile phones, emergency response systems, and the state's largest bank were all targeted. In addition, a concentrated attack effort was aimed at the offices of the president, prime minister, parliament, and the foreign ministry.[4]

The relevance of this attack, however, highlights some of the problems for developing an effective cyber deterrence system: even though Estonia intimated that it was able to trace some of the attacks to Russian government offices, it did not in fact establish any direct governmental links. Russia always maintained that the attacks came from renegade cyber nationalists, acting according to their own sense of warped patriotism but not on the orders of any official government office or agency. It is more a testimony to the state of global public perception that no one today believes the Russian version of the attacks and takes for granted the Estonian version—there never was a definitive "smoking gun" piece of evidence proving formal Russian governmental policy as the chief culprit in the Estonian attacks.

This is a perfect real-world example of the attribution problem often theorized by cyber specialists: it is often too difficult to accurately trace a cyber attack to its origin. Perhaps worse still, in cases where an origination point can at least be compellingly argued, there is still no definitive way of proving just who was "at the trigger point" launching the attack. Solving both of these issues would be essential for the development of a truly effective cyber deterrence system. An inability to prove culpability severely hampers any efforts to enact defensive measures. It really is as simple as "how do you know who to retaliate against if you cannot be sure who threw the virtual punch?" You cannot, and as a consequence any effort to build an effective cyber deterrence system emerges already deeply compromised.

Chinese Reality

Perhaps the only other state associated with cyber attacks and cyber espionage today as much as the Russian Federation is China. As early as the late 1990s the United States accused China of attacking various governmental agencies and attempting to infiltrate American nuclear facilities. Around the time Estonia was being attacked and accusing Russia, Germany had several infiltrations into governmental agencies and placed blame on China. Just as with the Estonian case, both the United States and Germany,

despite their adamant conviction of knowing who to blame, did not in fact have any real evidence linking the Chinese government to the detected incursions.[5]

This is no small matter and not an issue of blame semantics. The international community's response to evidence of direct governmental involvement in a cyber attack against another state could very easily be to consider it an act of war, even if at the moment a war of lesser degree. Accurate attribution, therefore, is of highest importance, as it could lead to the commitment of military forces and expose a state to the most serious of consequences—battlefield casualties. Any cyber deterrence system must therefore be capable of overcoming the attribution problem to be relevant in the most important issue of all—state security. It is clear that the world, not just the United States, is currently incapable of devising a system that can overcome this problem.

Unlike Russia, which has always been extremely secretive about its cyber activities and steadfast in its denial of engaging in any state-sponsored cyber attacks, China has been surprisingly open about its belief in the need and appropriateness of establishing an army of cyber warriors. China actively recruits and facilitates support of some of its more brilliant, locally developed hackers, called "honkers." Unabashed in their virtual patriotism, honkers espouse a philosophy that "the best defense is a capable offense." They do not consider themselves necessarily employees of the government or members of the Chinese intelligence community; they simply believe that China needs to be protected from adversaries. If it is brought to their attention that another state or corporation is initiating harmful maneuvers against their country, then it is their obligation to respond in kind. Note that responding in kind is not simply stopping a cyber attack but rather formulating a retaliatory cyber strike that is in fact more intense and more comprehensive than the initial strike.

In some ways this reality gives argument to the possibility of cyber war existing above and beyond conventional war; not because conventional war will ever be obsolete or be a state's most supreme form of security, but rather cyber war can be seen by many states as a less confrontational and more results-oriented maneuver. Effective hacking and strategic cyber attacks at the moment still hold many more opportunities for hiding participation while successfully gaining economic, political, diplomatic, and military secrets. In simple cost-benefit calculations, cyber war is much more cost effective than conventional war, so it is arguable that its popularity

over time will grow exponentially. When considering the impotence of defensive systems tasked with stopping such efforts, cyber war as a concept is fundamentally complex, convoluted, and diffused by design. These characteristics would at least be challenged by an open and transparent cyber-MAD system in ways present cyber deterrence methods do not.

At the moment it is fair to assume that Chinese honkers are not explicitly attempting to create a cyber version of the nuclear-MAD theory, but this does not mean they have not created such a policy in their de facto actions. What seems inarguable is that China has decided there are no ethical considerations in the cyber realm. In fact, it is easy to see how a state could make the counterargument—if cyber war will not necessarily involve immediate and direct bloodshed due to the cyber attacks, then ethical handcuffs can be freely removed from state considerations. More importantly, China has given the rest of the world a theoretical blueprint justifying such a policy—the honkers' offensive philosophy is not based on any sense of vindictive bloodlust, but rather a careful calculation of what is truly effective in the cyber realm: defensive capabilities are hopelessly compromised; therefore, only offensive threats have the potential to deter enemy initiatives.

In some ways this thought process has already been supported by none other than the current vice-chairman of the Joint Chiefs of Staff, Gen James Cartwright, who argued in 2007 before the Strategic Forces Subcommittee of the Senate Armed Forces Committee that it was "time to apply the principles of warfare to the cyber domain . . . and the defense of the nation is better served by capabilities *enabling us to take the fight to our adversaries* when necessary to deter actions detrimental to our interests."[6] Cyber deterrence as it is currently being envisioned does not carry this capability and does not enable the United States to take the fight to adversaries. This is not an attempt to beat the reader incessantly with a dead cyber horse, but is rather the necessary emphasis on how the United States clings to defense. It seems determined to fit this square peg into a round hole, even if to its own security detriment. As politically uncomfortable as it may be to model something important to US national security after Chinese hackers, it is clear at the moment honkers are more openly and successfully applying the principles of warfare to the cyber domain. The United States, meanwhile, refuses to transparently engage and develop its own possibilities and capabilities and therefore remains the more vulnerable cyber target.

Countercyberspace

A fascinating development, perhaps inspired by the admonishment of General Cartwright, comes with the concept of *countercyberspace*, defined as "a function consisting of operations to attain and maintain a desired degree of cyberspace superiority by the destruction, degradation, or disruption of an enemy's capabilities to use cyberspace."[7] This work comes from a new conceptualization of Air Force basic doctrine and is an admission of the need to produce new thinking (though arguably through the application of tried and true old-war ideas) to the realm of cyberspace and its defense. The issue at hand is of course trying to establish "cyberspace superiority," which AF Doctrine Document 2-11, "Cyberspace Operations," draft version defined as "the degree of advantage possessed by one force over another that permits the conduct of operations in cyberspace at a given time and place without prohibitive interference by the opposing force."[8] When taking these concepts and definitions into consideration, it becomes starkly clear how ineffective cyber deterrence will always be as long as it is a system constructed from defensive priorities. In the cyber realm a defensive system by default puts a state back on its governmental heels and does not contain the potential to conduct operations without prohibitive interference. America's cyber doctrine must achieve this capability.

In May 2007, President Bush ordered the National Security Agency (NSA) to conduct a cyber attack against cell phones and computer networks that Iraqi insurgents had used or intended to use in roadside bombings. The NSA complied, and its subsequent success essentially knocked out what was up to then an effective insurgent communications network. Many military analysts credit that effort with being monumental in turning the tide of the war.[9] It is true a cyber MAD cannot be exactly like nuclear MAD. It is not semantics when destruction is replaced by debilitation. So, while the analogy may not match up perfectly, it does work effectively, based on the fact that war in the twenty-first century has arguably moved away from being global and apocalyptic to something more regional and temporarily damaging. As such, the weapons in a cyber-MAD policy do not destroy states to sand and glass but simply cripple and incapacitate them across realms that are crucial to their effective functioning and governance. Such damage is not insignificant.

Clearly, the United States has the technical capability and the strategic aggressiveness to conduct such operations. It must now conceptualize an offensive mind-set to begin defending cyberspace. The problem to this

point has been its relatively limited sphere of utilization—the Iraqi example was a case of open and explicit war aimed at a target that was actively and aggressively attacking American military personnel. Granted, this may not be as politically clean, but it can be dramatically more effective in limiting adversaries who are motivated to attack the United States or other countries across the virtual commons. Keep in mind that in the twenty-first century, cyberspace is no lesser space to guard. It is true news media will not be able to show body counts or bloody battlefields when a country is victim to a massive cyber attack, but the devastation and destruction of such an attack in many ways can be more comprehensive and far-reaching.

Lacking Infrastructure

The logical arguments for a cyber-MAD policy become even more compelling when the technical obstacles facing a true defensive cyber deterrence are examined in full. For the past 10 years the United States has invested heavily in cyber-security technologies. Despite this commitment and investment, major problems remain across the most fundamental areas. There is still no large-scale deployment of security technology capable of comprehensively protecting vital American infrastructure.[10] The need for new security technologies is essential, but to date the best developments have only been in the small-to-medium-scale private research facilities. What would be required to make rapid, large-scale advances in new network security mechanisms is daunting:

- development of large-scale security test beds, combined with new frameworks and standards for testing and benchmarking;
- overcoming current deficiencies and impediments to evaluating network security mechanisms, which to date suffer from a lack of rigor;
- relevant and representative network data;
- adequate models of defense mechanisms; and
- adequate models of the network and for background and attack traffic data.

Most of these issues are problematic because of the severe complexity of interactions between traffic, topology, and protocols.[11] In short, it is simply easier to attack than to defend in the cyber realm, and the innate com-

plexities of infrastructure preparedness make it seem likely this is not just an estimation of current affairs but rather an axiom that will stand across eras. Hackers will always trump defenders. The United States must not waste time attacking the virtual windmill when it already has the technology, talent, and capability to create a different policy path.

One counterargument to this rejects that the cyber realm will remain inherently dominated by offensive capabilities. The most often praised defensive measures that are allegedly catching up to offensive threats (IPV-6 and gateway technologies) are unfortunately a bit of an overstatement, as the cyber arena is never static—whatever defensive countermeasures are developed, one can rest assured there will be answers to those measures. And offensive answers so far have always outpaced the defensive "improvements." There is nothing in the foreseeable future that seems to truly challenge this basic reality. The United States should indeed continue to develop, improve, and refine its defensive technologies. But it should not be so naïve as to think it will ever be capable of developing a defensive deterrence that will continuously and routinely outwork and outmaneuver offensive threats. It simply does not seem that the structure of the cyber realm will allow this reality to emerge.

The Asymmetric Nature of Cyber Warfare

The United States' failure to enter the cyber arena offensively, as a reflection of open and transparent policy (or even to create the perception of willingness to offensively engage), has only exacerbated the asymmetric nature of cyber attacks. The commercialization, standardization, and low cost of high technology around the globe make waging cyber campaigns dramatically more simplistic than defending against them. Quite literally a dozen determined programmers are capable of threatening the US logistics network, stealing operational plans, blinding intelligence capabilities, or hindering the ability to deliver weapons on target.[12] This was never more obvious than in 2008, when the Department of Defense suffered a significant intrusion into its supposedly secured military networks. An infected flash drive was inserted into a military laptop in the Middle East. Placed there by a foreign intelligence agency, the drive succeeded in releasing malicious computer code that was able to spread so far and so deep into classified and unclassified information that it was considered akin to establishing a "digital beachhead."[13]

These examples perfectly illustrate the potential nastiness and futility of fighting against asymmetry. This is an innate structural problem that cannot be overcome, because of the nature of technology and the free market. The Internet was designed to be open and accessible, not only for ease of use among the most basic of consumers but also to encourage and foster low barriers to innovation. As a consequence, offense will always have the upper hand.[14] But instead of letting the logic of this reality lead America into a new conceptualization of "offensive defense," the thinking of the United States is entrenched in a defensive mind-set that can only result in a compromised system of deterrence.

Though asymmetry makes staying ahead of attacking adversaries highly doubtful, Lynn argues that this only emphasizes the need for the United States to be more adaptable to constantly adjust and improve its defenses. He even says that old, Cold War traditions of deterrence (models of assured retaliation) will *not* work in cyberspace due to the aforementioned attribution problem, making it nearly impossible to know just who to retaliate against. Therefore, deterrence is supposed to be about successfully denying the benefits to an attacker, rather than trying to impose costs through aggressive retaliation.[15]

While this article testifies to the problem of attribution, this does not lead to an argument for moving away from old models of retaliatory deterrence but actually the reverse: a retaliatory cyber model would not be about who to launch missiles against, but rather enforcing the perception of massive technological/infrastructural debilitation if even the suspicion of an attack is determined and attributed. Nuclear MAD was successful not because various states actually launched nuclear weapons; it succeeded because of the conviction across all parties that an attack of this nature would be so universally destructive that the cost far outweighed any potential benefits. A cyber-MAD model has to operate on this same principle, only with virtual weapons rather than kinetic ones. If done successfully, essentially weaponizing the cyber doctrine of the United States, then it becomes prohibitively expensive for an adversary to risk an attack.

This is not in fact arguing for the creation of some cyber variant of a Dr. Strangelove doomsday machine, the repercussions of which would solve the attribution problem. Taken to its extreme extrapolation, a cyber-MAD policy does deter as nuclear MAD—the perception of realistic virtual devastation via retaliatory strike does induce fear of action, thereby rendering the global system safe through dangerous, but stable, equilibrium. Just as

with nuclear weapons, the ability to universally destroy the virtual commons cannot be the ultimate hope for peace across the system. This is not an argument for giving the president a choice between surrender or hacking the modern world into the Middle Ages. Rather, a cyber-MAD policy—by being open, transparent, mutual, and offensive—would have enough new deterrents built into it structurally to not only provide more options but also give pause to rogue behavior that might probe its edges.

Recall that mutuality not only builds fear but this same fear also allows the possibility of trust through repeated engagement. Up to now the dynamic nature of the cyber realm too heavily favored those who would do damage against it. Cyber MAD would finally put some of that dynamism in the hands of major powers with a mutual interest in rules, regulations, and stability.

Cyberwar, Cyber Deterrence, and Political Complexity

Trying to study the consequences of the cyber realm's impact on war and conflict is a hornet's nest of political complications. Even when trying to develop a purely defensive, non-attacking system of protection, there is a preponderance of complex considerations. How can one be sure of the attacker? Can assets be held at risk when under suspicion of a cyber attack? Does retaliation send the right message to the defending side? Should there be a threshold for a response? How do you avoid escalation?[16] All of these questions pose problems not just because they are complicated but because the nature of a defensive cyber system exacerbates the flaws within such policy rather than eliminating them, and yet other questions arguably emerge only because of these inherent flaws in a defensive mind-set.

Complexity is reduced when considering the development of a cyber-MAD policy, but admittedly it may place the United States in an uncomfortable political position at first. Consider just war theory. In the first instance, jus ad bellum, when states may lawfully consider going from peace to war, there are at least three immediate criteria most states would prefer to have on their side: right purpose, duly constituted authority, and last resort.[17] A cyber-MAD policy would be especially harsh on each criterion: the policy does not operate on only going to war in self-defense, since the nature of cyber security precludes any real notion of being able to effectively defend against a massive cyber attack; there is also the risk of cyber MAD circumventing proper governmental notification because total

debilitation would depend in large part on the element of surprise, which works against premeditated transparency and openness; and finally, cyber MAD by its very nature is the antithesis of last resort—the effectiveness of the position comes from not being purely retaliatory but potentially preemptive, indicating a willingness to use virtual weapons in more than just desperate circumstances.

Many would argue that from a purely political/diplomatic perspective these positions appear somewhat untenable. This would be true if cyber MAD were set up structurally so that the United States dominates these offensive capabilities alone and de facto, becoming a virtual tyrant vis-à-vis the other great powers. But as argued earlier, the inherent structure of the cyber realm makes such a goal, even if logical for a great power, highly unlikely and nearly impossible. Therefore, all states pursuing cyber MAD would be relatively equal in their weaponization efforts. This allows for the possibility over time for the perception of equal debilitation to take effect and arguably create similar deterrence stimuli as nuclear MAD.

The initial political and diplomatic discomfort associated with cyber MAD does not improve when considering jus in bello, or the desire to have states maintain principles of justice while in war. Again, three main criteria can be highlighted: noncombatant immunity, proportionality, and more good than harm.[18] A cyber-MAD policy would still have the major benefit of any cyber defense system: that it is relatively bloodless. However, the benefit does start to become more ambiguous under cyber MAD; a massive strike against a state's infrastructure, debilitating important societal mechanisms and functions, would almost certainly result in noncombatant suffering and thereby not guarantee immunity in the most formal sense. Proportionality clearly cannot be met simply because the point of a cyber-MAD policy would be to secure defense through retaliatory second-strike *nonproportionality.* It would be the guarantee of that nonproportional response/strike that would bring about the deterring impulse. Finally, the criterion of more good than harm under cyber MAD really would be, in the end, a completely arbitrary interpretation based on which side and whose security goals were being considered.

Little work has been done to date on an explicit conceptualization of an offensive and transparent cyber strategy to heighten national security. What has been done achieves a general consensus that there are three obvious ways a state could create the capability to inflict damage on another state or nonstate adversary via cyber attack. The first option is simply creating

the capability through one's own forces and technologies. The second is to cultivate a volunteer force that can be guided to attack designated targets with little or no attribution to the supporting government. The third option is to outsource at least parts of the problem to other governments, commercial entities, or criminal underworld organizations in a quasi-mercenary model.[19] Each option clearly carries its own flaws.

Both China and Russia formally and informally dabble with options one and two. States like Iran, North Korea, and Nigeria have been at least cursorily connected to option three. Perhaps this is the largest difficulty impacting the politics of American policymaking—it seems plausible that the United States is simply reluctant to consider a shift in policy that would so clearly associate it with this group of countries, no matter what the advantages. Of the three options, option one has the best chance of consideration by the United States, as this homegrown policy would at least be arguably controllable and explicitly defined by American democratic institutions with their inherent checks and balances informed by principles of transparency and accountability.

The United States does indeed have the capability of developing cadres assigned to the task of developing a weaponized cyber realm. But where this has been done so far has been on a small scale and in highly classified areas. These characteristics make it an obvious *attacking* capability structured most effectively for use in the context of open aggression and war rather than as it is ultimately needed—as a *deterring* capability meant to prevent said aggression from occurring during times of peace. Again, the greatest advantage with cyber MAD is not in truly achieving a *usable* second-strike capability but in creating over time the believability in such retaliation so the second strike is never required.

The other two options afford no such chance of a truly governable, accountable policy and are not likely to be considered by the United States. This article does not challenge the premise that initially a cyber-MAD policy would place the United States in some rather awkward political positions. Rather, it takes the more quintessentially Machiavellian position that national security is best managed by efficacy and control, even at the expense of diplomatic image and public perceptions of righteousness.

Conclusion

Most analysts, military specialists, and government officials admit that life in the twenty-first century will include cyber attacks. There is no vision of a world free from such attacks. This simple admission undermines the efficacy of a cyber deterrence system whose reason for being is the prevention of such attacks. This article is not so contrarian as to argue anarchically for abandonment of the effort to achieve real cyber security. Rather it asks that certain structural realities finally be given equal intellectual space at the discussion table and allow that space to entertain new options and possibilities. There are two structural realities in particular that should be emphasized. First, in the cyber realm offense always dominates and always will. It is structural and axiomatic. Second, the capabilities, technology, and talent already exist to institute this system within the United States. What is needed is a change in mind-set and encouraging new ideas and policies—transparently. Not easy by any means, but still achievable.

The imposition of a cyber-MAD policy could prove more effective, even though it may make the United States uncomfortable politically and diplomatically. The debate continues and the argument remains: greater cyber security can be achieved by mutually assured debilitation for all. SSQ

Notes

1. Mark Young, "National Cyber Doctrine: The Missing Link in the Application of American Cyber Power," *Journal of National Security Law and Policy* 4, no. 1 (2010): 173–96.
2. Ibid.
3. Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009).
4. Arthur Bright, "Estonia Accuses Russia of Cyberattack," *Christian Science Monitor*, 17 May 2007, http://www.csmonitor.com/2007/0517/p99s01-duts.html.
5. Alan W. Dowd, "Are We Ready for WWI?" *Fraser Forum,* September 2009, 12–14.
6. James Cartwright, "Statement before the Strategic Forces Subcommittee of the Senate Armed Services Committee," 28 March 2007.
7. Eric D. Trias and Bryan M Bell, "Cyber This, Cyber That . . . So What?" *Air and Space Power Journal* 24, no. 1 (Spring 2010): 90–100.
8. Ibid.
9. Ibid.
10. Ruzena Bajcsy et al., "Cyber Defense Technology Networking and Evaluation," *Communications of the Association of Computing Machinery* 47, no. 3 (March 2004): 58–61.
11. Ibid.
12. William J. Lynn, "Defending a New Domain," *Foreign Affairs* 89, no. 5 (September/October 2010).
13. Ibid.
14. Ibid.

15. Ibid.

16. Libicki, *Cyberdeterrence and Cyberwar.*

17. Andrew Liaropoulos, "War and Ethics in Cyberspace: Cyber-Conflict and Just War Theory," *Proceedings of the 9th European Conference on Information Warfare and Security* (Reading, UK: Academic Publishing, Ltd., 2010), 177–82.

18. Ibid.

19. Rain Ottis, "Theoretical Model for Creating a Nation-State Level Offensive Cyber Capability," *Proceedings of the 8th European Conference on Information Warfare and Security* (Reading, UK: Academic Publishing, Ltd., 2009), 177–82.

Nuclear Crisis Management and "Cyberwar"

Phishing for Trouble?

Stephen J. Cimbala

If the ultimate weapons of mass destruction, nuclear weapons, and the supreme weapons of soft power, information warfare, are commingled during a crisis, the product of the two may be an entirely unforeseen and unwelcome hybrid. Crises by definition are exceptional events. No Cold War crisis took place between states armed with advanced information weapons *and* with nuclear weapons. But given the durability of the two trends—interest in infowar and in nuclear weapons—the potential for overlap and its implications for nuclear crisis management deserve further study and policy consideration. The discussion below proceeds toward that end, by looking at relevant concepts and examples including information warfare, crisis management, the link between cyberwar and nuclear crisis management, and its implications.

Information Warfare

Information warfare can be defined as activities by a state or nonstate actor to exploit the content or processing of information to its advantage in time of peace, crisis, or war and to deny potential or actual foes the ability to exploit the same means against itself.[1] This is an expansive, and permissive, definition, although it has an inescapable bias toward military- and security-related issues.[2] Information warfare can include both cyberwar and netwar. *Cyberwar*, according to John Arquilla and David Ronfeldt, is a comprehensive, information-based approach to battle, normally discussed in terms of high-intensity or mid-intensity conflict.[3] *Netwar* is defined by the same authors as a comprehensive, information-based approach

Stephen J. Cimbala, PhD, is Distinguished Professor of Political Science at Penn State University–Brandywine. Dr. Cimbala is the author of numerous works in the fields of national security policy, nuclear arms control, and other topics. The award-winning Penn State teacher has also served as a consultant for various US government agencies and private contractors. His recent publications include *The George W. Bush Defense Program* (Potomac Publishers) and, with Peter Forster, *Multinational Military Intervention* (Ashgate).

to societal conflict. Cyberwar is more the province of states and conventional wars; netwar more characteristic of nonstate actors and unconventional wars.[4]

Cyberwar is distinct from the problem of deterrence, although there are obvious "real world" overlaps. The concept of "cyber deterrence" involves degrees of uncertainty and complexity, including a leap of analytic faith beyond what we know about conventional or nuclear deterrence. Cyber attacks generally obscure the identity of the attackers, can be initiated from outside of or within the defender's state territory, are frequently transmitted through third parties without their complicity or knowledge, and can sometimes be repeated almost indefinitely by skilled attackers, even against agile defenders. In addition, the contrast between the principles of cyber deterrence and nuclear deterrence encourages modesty in the transfer of principles from the latter to the former.[5]

Added to this is the civil-military interaction that will take place between designated military cyber samurai and their civilian DoD (and other) superiors in the chain of command who may be cyber-challenged or even pre-cyber in their understanding of information technology and its impacts. The nexus among new information capabilities, their implications for decision making, and their potential vulnerabilities to attack may be comprehended by a select few, if at all. But politics will ultimately drive all strategy—including cyber strategy—for better or worse. At its apex, strategy is the bridge that connects political objectives with military operations, whether digital or kinetic.[6]

Crisis Management—Nuclear and Other

Crisis management, including nuclear crisis management, is both a competitive and cooperative endeavor between military adversaries. A *crisis* is, by definition, a time of great tension and uncertainty.[7] Threats are imminent, and time pressure on policymakers seems intense. Each side has objectives it wants to attain and values it deems important to protect. During a crisis, state behaviors are especially interactive and interdependent with those of another state. It would not be far-fetched to refer to this interdependent stream of interstate crisis behaviors as a system, provided the term *system* is not understood as an entity completely separate from the state or individual behaviors that comprise it. The system aspect

implies reciprocal causation of the crisis behaviors of "A" by "B," and vice versa.

One aspect of crisis management is the deceptively simple question: What defines a crisis as such? When does the latent capacity of the international order for violence or hostile threat assessment cross over into the terrain of actual crisis behavior? A breakdown of general deterrence in the system raises threat perceptions among various actors, but it does not guarantee that any particular relationship will deteriorate into specific deterrent or compellent threats. Patrick Morgan's concept of "immediate" deterrence failure is useful in defining the onset of a crisis: specific sources of hostile intent have been identified by one state with reference to another, threats have been exchanged, and responses must now be decided upon.[8] The passage into a crisis is equivalent to the shift from Hobbes' world of omnipresent potential for violence to the actual movement of troops and exchanges of diplomatic demarches.

All crises are characterized to some extent by a high degree of threat, short time for decision, and a "fog of crisis" reminiscent of Clausewitz's "fog of war" that confuses crisis participants about what is happening. Before the discipline of crisis management was ever invented by modern scholarship, historians had captured the rush-to-judgment character of much crisis decision making among great powers.[9] The influence of nuclear weapons on crisis decision making is therefore not easy to measure or document, because the avoidance of war can be ascribed to many causes. The presence of nuclear forces obviously influences the degree of destruction that can be done should crisis management fail. Short of that catastrophe, the greater interest of scholars is in how the presence of nuclear weapons might affect the decision-making process itself in a crisis. The problem is conceptually elusive: there are so many potentially important causal factors relevant to a decision with regard to war or peace. History is full of dependent variables in search of competing explanations.

Another question involves the "level of analysis" problem for explanations of, and predictions about, crisis management. Who, for example, is likely to be affected by cyber attacks during a nuclear crisis? Disruption of communications or data flows to enemy senior policymakers and force commanders is a candidate stratagem for an attacker. But the head of the snake is not necessarily the most vulnerable part of a bureaucracy or political system. Advanced nuclear powers will have both political orders of succession and delegations of military command authority in place against

decapitation attacks. Cyber mischief might be more efficiently targeted on the opponent's civilian infrastructure, including that part of the civilian infrastructure that overlaps with military use. An example of this kind of attack would be efforts to disrupt information or communication flows in the electrical power grids or financial systems of another state by means of viruses, Trojan horses, botnets, distributed denial-of-service (DDOS) attacks, or other deceptive or destructive measures.

Cyber strikes could also be aimed directly at the opponent's nuclear infrastructure in time of peace or war. For example, the "Stuxnet" virus that attacked Iran's nuclear facilities in 2010 was assumed by some to have been created by Israel and/or the United States. According to a German computer expert who was among the first to analyze the Stuxnet code, the virus (or worm) may have set back Iran's nuclear program by two years. Describing the Stuxnet worm as the most "advanced and aggressive malware in history," the German expert added, "This was nearly as effective as a military strike, but even better since there are no fatalities and no full-blown war."[10] This cyber attack took place in "peacetime" and reportedly will require considerable time and effort for Iran to remove the virus, replace affected computer equipment, and rebuild centrifuges at its uranium enrichment facility at Natanz.[11]

Suppose an attack of this nature had been attempted by unknown parties after Iran had already become a nuclear weapons state and entered into a crisis with Israel. And the phrase "unknown parties" is not an idle one. Third parties could conceivably use cyber strikes to provoke catalytic wars between two rivals—say, for example, Serbians or Balts firing cyber bullets into a Russo-Georgian clash or Japanese or Chinese hackers cyber surfing during a war between North and South Korea. The sources of third-party disruption (either condoned by governments or based on freelancers with their own political agendas) against a colliding dyad of state actors could also be nonstate actors—including terrorists, criminals, or "super-empowered individuals"—piggybacking on crises for their own reasons.[12] Nor is it inconceivable that during a crisis two disputants or third parties might fire up their own equivalents of WikiLeaks and disclose potentially incriminating details about other states' policymaking or force planning, or about their leaders' personality flaws. Throw "NikiLeaks" into the Cuban missile crisis or "GorbyLeaks" into the August 1991 failed putsch in Moscow, and stir the historically counterfactual mix.

Attributes for Successful Crisis Management

The first requirement of successful crisis management is communications transparency. Transparency includes clear signaling and undistorted communications. Signaling refers to the requirement that each side must send its estimate of the situation to the other. It is not necessary for the two sides to have identical or even initially complementary interests. But a sufficient number of correctly sent and received signals are prerequisite to effective transfer of enemy goals and objectives from one side to the other. If signals are poorly sent or misunderstood, steps taken by the sender or receiver may lead to unintended consequences, including miscalculated escalation.

Communications transparency also includes high-fidelity communication between adversaries and within the respective decision-making structures of each side. High-fidelity communication in a crisis can be distorted by everything that might interfere physically, mechanically, or behaviorally with accurate transmission. Electromagnetic pulses that disrupt communication circuitry or physical destruction of communication networks are obvious examples of impediments to high-fidelity communication. Cultural differences that prevent accurate understanding of shared meanings between states can confound deterrence as practiced according to one side's theory. As Keith Payne notes, with regard to the potential for deterrence failure in the post–Cold War period:

> Unfortunately, our expectations of opponents' behavior frequently are unmet, not because our opponents necessarily are irrational but because we do not understand them—their individual values, goals, determination, and commitments—in the context of the engagement, and therefore we are surprised when their "unreasonable" behavior differs from our expectations.[13]

A second requirement of successful crisis management is reducing time pressure on policymakers and commanders so no unintended, provocative steps are taken toward escalation mainly or solely as a result of a misperception that "time is up." Policymakers and military planners are capable of inventing fictive worlds of perception and evaluation in which "H-hour" becomes more than a useful benchmark for decision closure. In decision pathologies possible under crisis conditions, deadlines may be confused with policy objectives themselves: ends become means, and means, ends. For example: the war plans of the great powers in July 1914 contributed to a shared self-fulfilling prophecy among leaders in Berlin, St. Petersburg, and Vienna that only by prompt mobilization and attack could decisive

losses be avoided in war. Plans predicated on the determinism of mobilization timetables proved insufficiently adaptive for policymakers who wanted to slow down the momentum of late July and early August toward an irrevocable decision in favor of war.

One result of compressing the decision time in a crisis, compared to typical peacetime patterns, is that the likelihood of Type I (undetected attack) and Type II (falsely detected attack) errors increases. Tactical warning and intelligence networks grow accustomed to the routine behavior of other state forces and may misinterpret nonroutine behavior. Unexpected surges in alert levels or uncharacteristic deployment patterns could trigger misreadings of indicators by tactical operators. As Bruce Blair has argued:

> In fact, one distinguishing feature of a crisis is its murkiness. By definition, the Type I and Type II error rates of the intelligence and warning systems rapidly degrade. A crisis not only ushers in the proverbial fog of crisis symptomatic of error-prone strategic warning but also ushers in a fog of battle arising from an analogous deterioration of tactical warning.[14]

A third attribute of successful crisis management is that each side should be able to offer the other a safety valve or a face-saving exit from a predicament that has escalated beyond its original expectations. The search for options should back neither crisis participant into a corner from which there is no graceful retreat. For example, during the Cuban missile crisis of 1962, President Kennedy was able to offer Soviet premier Khrushchev a face-saving exit from his overextended missile deployments. Kennedy publicly committed the United States to refrain from future military aggression against Cuba and privately agreed to remove and dismantle Jupiter medium-range ballistic missiles previously deployed among its NATO allies.[15] Kennedy and his inner circle recognized, after some days of deliberation and clearer focus on the Soviet view of events, that the United States would lose, not gain, by a public humiliation of Khrushchev that might, in turn, diminish Khrushchev's interest in any mutually agreed solution to the crisis.

A fourth attribute of successful crisis management is that each side maintains an accurate perception of the other's intentions and military capabilities. Clarity of perception becomes difficult during a crisis because, in the heat of a partly competitive relationship and a threat-intensive environment, intentions and capabilities can change. Robert Jervis warned that Cold War beliefs in the inevitability of war might have created a self-fulfilling prophecy:

> The superpowers' beliefs about whether or not war between them is inevitable create reality as much as they reflect it. Because preemption could be the only rational reason to launch an all-out war, beliefs about what the other side is about to do are of major importance and depend in large part on an estimate of the other's beliefs about what the first side will do.[16]

Intentions can change during a crisis if policymakers become more optimistic about gains or more pessimistic about potential losses during the crisis. Capabilities can change due to the management of military alerts and the deployment or other movement of military forces. Heightened states of military readiness on each side are intended to send a two-sided signal: of readiness for the worst if the other side attacks, and of a nonthreatening steadiness of purpose in the face of enemy passivity. This mixed message is hard to send under the best of crisis management conditions, since each state's behaviors and communications, as observed by its opponent, may not seem consistent. Under the stress of time pressures and of military threats, different parts of complex security organizations may be making decisions from the perspective of their narrowly defined, bureaucratic interests. These bureaucratically chosen decisions and actions may not coincide with the policymakers' intent, nor with the decisions and actions of other parts of the government. As Alexander George has explained:

> It is important to recognize that the ability of top-level political authorities to maintain control over the moves and actions of military forces is made difficult because of the exceedingly large number of often complex standing orders that come into effect at the onset of a crisis and as it intensifies. It is not easy for top-level political authorities to have full and timely knowledge of the multitude of existing standing orders. As a result, they may fail to coordinate some critically important standing orders with their overall crisis management strategy.[17]

As policymakers may be challenged to control numerous and diverse standard operating procedures, political leaders may also be insufficiently sensitive to the costs of sudden changes in standing orders or unaware of the rationale underlying those orders. For example, heads of state or government may not be aware that more permissive rules of engagement for military forces operating in harm's way come into play once higher levels of alert have been authorized.[18]

Cyberwar plus Nuclear Crisis Management

This section discusses how cyberwar might adversely affect nuclear crisis management. Readers are advised, however, that history is indeterminate. It might turn out that, in some fortuitous cases, the United States could use nuclear deterrence and cyberwar as joint multipliers toward a successful outcome in crisis or war. For example, in facing down an opponent with a comparatively small or no nuclear arsenal and inferior conventional strike capabilities, the United States or another power could employ information warfare aggressively "up front" while forgoing explicit mention of its available nuclear capability. Russia's five-day war against Georgia in August 2008 involved obvious cyber attacks as well as land and air operations, but no explicit nuclear threats. On the other hand, had Georgia already been taken into membership by NATO prior to August 2008 or had Russo-Georgian fighting spread into NATO member-state territory, the visibility of Russia's nuclear arsenal as a latent and potentially explicit threat would have been much greater.

Notwithstanding the preceding disclaimers, information warfare has the potential to attack or disrupt successful crisis management on each of four dimensions. First, it can muddy the signals being sent from one side to the other in a crisis. This can be done deliberately or inadvertently. Suppose one side plants a virus or worm in the other's communications networks.[19] The virus or worm becomes activated during the crisis and destroys or alters information. The missing or altered information may make it more difficult for the cyber victim to arrange a military attack. But destroyed or altered information may mislead either side into thinking that its signal has been correctly interpreted when it has not. Thus, side A may intend to signal "resolve" instead of "yield" to its opponent on a particular issue. Side B, misperceiving a "yield" message, may decide to continue its aggression, meeting unexpected resistance and causing a much more dangerous situation to develop.

Infowar can also destroy or disrupt communication channels necessary for successful crisis management. One way it can do this is to disrupt communication links between policymakers and military commanders during a period of high threat and severe time pressure. Two kinds of unanticipated problems, from the standpoint of civil-military relations, are possible under these conditions. First, political leaders may have predelegated limited authority for nuclear release or launch under restrictive conditions; only when these few conditions obtain, according to the

protocols of predelegation, would military commanders be authorized to employ nuclear weapons distributed within their command. Clogged, destroyed, or disrupted communications could prevent top leaders from knowing that military commanders perceived a situation to be far more desperate, and thus permissive of nuclear initiative, than it really was. During the Cold War, for example, disrupted communications between the US National Command Authority and ballistic missile submarines, once the latter came under attack, could have resulted in a joint decision by submarine officers to launch in the absence of contrary instructions.

Second, information warfare during a crisis will almost certainly increase the time pressure under which political leaders operate. It may do this literally, or it may affect the perceived timelines within which the policymaking process can make its decisions. Once either side sees parts of its command, control, and communications (C^3) system being subverted by phony information or extraneous cyber noise, its sense of panic at the possible loss of military options will be enormous. In the case of US Cold War nuclear war plans, for example, disruption of even portions of the strategic C^3 system could have prevented competent execution of parts of the SIOP (the strategic nuclear war plan). The SIOP depended upon finely orchestrated time-on-target estimates and precise damage expectancies against various classes of targets. Partially misinformed or disinformed networks and communications centers would have led to redundant attacks against the same target sets and, quite possibly, unplanned attacks on friendly military or civilian installations.

A third potentially disruptive effect of infowar on nuclear crisis management is that it may reduce the search for available alternatives to the few and desperate. Policymakers searching for escapes from crisis denouements need flexible options and creative problem solving. Victims of information warfare may have a diminished ability to solve problems routinely, let alone creatively, once information networks are filled with flotsam and jetsam. Questions to operators will be poorly posed, and responses (if available at all) will be driven toward the least common denominator of previously programmed standard operating procedures. Retaliatory systems that depend on launch-on-warning instead of survival after riding out an attack are especially vulnerable to reduced time cycles and restricted alternatives:

> A well-designed warning system cannot save commanders from misjudging the situation under the constraints of time and information imposed by a posture of

> launch on warning. Such a posture truncates the decision process too early for iterative estimates to converge on reality. Rapid reaction is inherently unstable because it cuts short the learning time needed to match perception with reality.[20]

The propensity to search for the first available alternative that meets minimum satisfactory conditions of goal attainment is strong enough under normal conditions in nonmilitary bureaucratic organizations.[21] In civil-military command and control systems under the stress of nuclear crisis decision making, the first available alternative may quite literally be the last; or so policymakers and their military advisors may persuade themselves. Accordingly, the bias toward prompt and adequate solutions is strong. During the Cuban missile crisis, a number of members of the presidential advisory group continued to propound an air strike and invasion of Cuba during the entire 13 days of crisis deliberation. Had less time been available for debate and had President Kennedy not deliberately structured the discussion in a way that forced alternatives to the surface, the air strike and invasion might well have been the chosen alternative.[22]

Fourth and finally on the issue of crisis management, infowar can cause flawed images of each side's intentions and capabilities to be conveyed to the other, with potentially disastrous results. Another example from the Cuban crisis demonstrates the possible side effects of simple misunderstanding and noncommunication on US crisis management. At the most tense period of the crisis, a U-2 reconnaissance aircraft got off course and strayed into Soviet airspace. US and Soviet fighters scrambled, and a possible Arctic confrontation of air forces loomed. Khrushchev later told Kennedy that Soviet air defenses might have interpreted the U-2 flight as a prestrike reconnaissance mission or as a bomber, calling for a compensatory response by Moscow.[23] Fortunately Moscow chose to give the United States the benefit of the doubt in this instance and to permit US fighters to escort the wayward U-2 back to Alaska. Why this scheduled U-2 mission was not scrubbed once the crisis began has never been fully revealed; the answer may be as simple as bureaucratic inertia compounded by noncommunication down the chain of command by policymakers who failed to appreciate the risk of "normal" reconnaissance under these extraordinary conditions.

Further Issues and Implications

The outcome of a nuclear crisis management scenario influenced by information operations may not be a favorable one. Despite the best efforts of crisis participants, the dispute may degenerate into a nuclear first use or first strike by one side and retaliation by the other. In that situation, information operations by either, or both, sides might make it more difficult to limit the war and bring it to a conclusion before catastrophic destruction and loss of life had taken place. Although there are no such things as "small" nuclear wars, compared to conventional wars, there can be different kinds of "nuclear" wars in terms of their proximate causes and consequences.[24] Possibilities include a nuclear attack from an unknown source; an ambiguous case of possible, but not proved, nuclear first use; a nuclear "test" detonation intended to intimidate but with no immediate destruction; and a conventional strike mistaken, at least initially, for a nuclear one. As George Quester has noted:

> The United States and other powers have developed some very large and powerful conventional warheads, intended for destroying the hardened underground bunkers that may house an enemy command post or a hard-sheltered weapons system. Such "bunker-buster" bombs radiate a sound signal when they are used and an underground seismic signal that could be mistaken from a distance for the signature of a small nuclear warhead.[25]

The dominant scenario of a general nuclear war between the United States and the Soviet Union preoccupied Cold War policymakers, and under that assumption concerns about escalation control and war termination were swamped by apocalyptic visions of the end of days. The second nuclear age, roughly coinciding with the end of the Cold War and the demise of the Soviet Union, offers a more complicated menu of nuclear possibilities and responses.[26] Interest in the threat or use of nuclear weapons by rogue states, by aspiring regional hegemons, or by terrorists abetted by the possible spread of nuclear weapons among currently nonnuclear weapons states stretches the ingenuity of military planners and fiction writers.

In addition to the world's worst characters engaged in nuclear threat of first use, there is also the possibility of backsliding in political conditions, as between the United States and Russia, or Russia and China, or China and India (among current nuclear weapons states). Politically unthinkable conflicts of one decade have a way of evolving into the politically unavoidable wars of another—World War I is instructive in this regard. The war between Russia and Georgia in August 2008 was a reminder that local

conflicts on regional fault lines between blocs or major powers have the potential to expand into worse.

If information operations might get in the way of de-escalation during a nuclear crisis, then why not just omit them? The political desire to do so conflicts with the military necessity for timely information gathering, assessment, and penetration of enemy networks to accomplish two necessary, but somewhat opposed, missions. First, each side would want to anticipate correctly the timing and character of the other's decision for nuclear first use—and, if possible, to throw logic bombs, Trojan horses, electronic warfare, or other impediments in the way (or if finesse is not preferred, bombing the relevant installations is always an option, although an obviously provocative one). The second, and somewhat opposed, mission is to communicate reliably with the other side one's preference for de-escalation, willingness to do so if reciprocity can be obtained, and awareness of the possibility that the situation will shortly get out of hand.

Conclusion

The objective of cyberwar in conventional conflicts is to deny enemy forces battlespace awareness and to obtain dominant awareness for oneself, as the United States largely was able to do in the Gulf War of 1991.[27] In a crisis with nuclear weapons available to the side against which infowar is used, crippling the foe's intelligence and command and control systems is an objective possibly at variance with controlling conflict and prevailing at an acceptable cost. And, under some conditions of nuclear crisis management, crippling the C^4ISR of the foe may be self-defeating. Whether nuclear or other deterrence can work in a particular cyber context is more dependent upon political, as opposed to military, variables. As Lawrence Freedman has noted, strategic studies have sometimes been too preoccupied with military capabilities and thus insufficiently sensitive to the point that "the balance of terror rests upon a particular arrangement of political relations as much as on the quantity and quality of the respective nuclear arsenals."[28] SSQ

Notes

1. Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009), argues that strategic cyberwar is unlikely to be decisive, although operational cyberwar has an important niche role. Libicki also warns that deterrence in the cyber realm is unlikely to behave as it does in

other domains, including conventional war and nuclear deterrence. See also Will Goodman, "Cyber Deterrence: Tougher in Theory than in Practice?" *Strategic Studies Quarterly* 4, no. 3 (Fall 2010): 102–35. Goodman argues that cyberspace poses unique challenges for deterrence but not necessarily impossible ones.

2. Concepts related to information warfare are discussed in David S. Alberts, John J. Garstka, Richard E. Hayes, and David T. Signori, *Understanding Information Age Warfare*, 3rd ed. (Washington: DoD, October 2004), esp. 53–94; and Alberts, Garstka, and Frederick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, 6th printing (Washington: DoD, April 2005), esp. 87–122. Col Thomas X. Hammes, USMC, retired, discusses the Pentagon's Joint Publication 3-13, *Information Operations*, and the DoD understanding of information in modern warfare in Hammes, "Information Warfare," chap. 4, in *Ideas as Weapons: Influence and Perception in Modern Warfare*, eds. G. J. David Jr. and T. R. McKeldin III (Washington: Potomac Books, 2009), 27–34. See also John Arquilla, *Worst Enemy: The Reluctant Transformation of the American Military* (Chicago: Ivan R. Dee, 2008), esp. chaps. 6–7. For perspective on the role of information operations in Russian military policy, see Timothy L. Thomas, "Russian Information Warfare Theory: The Consequences of August 2008," chap. 4, in *The Russian Military Today and Tomorrow: Essays in Memory of Mary Fitzgerald*, eds. Stephen J. Blank and Richard Weitz (Carlisle, PA: Strategic Studies Institute, US Army War College, July 2010); and Thomas, "Russia's Asymmetrical Approach to Information Warfare," chap. 5, in *The Russian Military into the Twenty-first Century*, ed. Stephen J. Cimbala (London: Frank Cass, 2001), 97–121.

3. Richard A. Clarke, former counterterrorism coordinator for the George W. Bush and Clinton administrations, and coauthor Robert K. Knake include both cyberwar and netwar activities, as defined by John Arquilla and David Ronfeldt in their concept of "cyber war." See Richard A. Clarke and Robert K. Knake, *Cyber War* (New York: HarperCollins, 2010). For an introduction to this topic, see John Arquilla and David Ronfeldt, "A New Epoch—and Spectrum—of Conflict," in *In Athena's Camp: Preparing for Conflict in the Information Age*, ed. Arquilla and Ronfeldt (Santa Monica: RAND, 1997), 1–22. See also, on definitions and concepts of information warfare, Martin C. Libicki, *What Is Information Warfare?* ACIS Paper 3 (Washington: National Defense University, August 1995); Libicki, *Defending Cyberspace and other Metaphors* (Washington: NDU, Directorate of Advanced Concepts, Technologies, and Information Strategies, February 1997); Arquilla and Ronfeldt, *Cyberwar Is Coming!* (Santa Monica: RAND, 1992); and David S. Alberts, *The Unintended Consequences of Information Age Technologies: Avoiding the Pitfalls, Seizing the Initiative* (Washington: NDU, Institute for National Strategic Studies, Center for Advanced Concepts and Technology, April 1996).

4. John Arquilla and David Ronfeldt, "The Advent of Netwar," in *In Athena's Camp*, 275–94. With regard to the tasks for US Cyber Command (established in 2009) and its implications for the national security decision-making process, see Wesley R. Andrues, "What U.S. Cyber Command Must Do," *Joint Force Quarterly*, issue 59 (4th Quarter 2010): 115–20.

5. Libicki, *Cyberdeterrence and Cyberwar*, xvi.

6. This concept is elegantly explained in Colin S. Gray, *The Strategy Bridge: Theory for Practice* (Oxford: Oxford University Press, 2010), esp. 96–120.

7. For pertinent concepts, see Alexander L. George, "A Provisional Theory of Crisis Management," in *Avoiding War: Problems of Crisis Management*, ed. Alexander L. George (Boulder, CO: Westview Press, 1991), 22–27, for the political and operational requirements of crisis management; and George, "Strategies for Crisis Management," ibid., 377–94, for descriptions of offensive and defensive crisis management strategies. See also Ole R. Holsti, "Crisis Decision Making," in *Behavior, Society and Nuclear War*, ed. Philip E. Tetlock et al. (New York: Oxford University Press, l989), I, 8–84; and Phil Williams, *Crisis Management* (New York: John Wiley

and Sons, 1976). See also George, "Coercive Diplomacy: Definition and Characteristics," in *The Limits of Coercive Diplomacy*, 2d ed., George and William E. Simons (Boulder, CO: Westview Press, 1994), esp. 8–9; and in the same volume, George, "The Cuban Missile Crisis: Peaceful Resolution through Coercive Diplomacy," 111–32.

8. See Patrick M. Morgan, *Deterrence: A Conceptual Analysis* (Beverly Hills, CA: Sage Publications, 1983); and Richard Ned Lebow and Janice Gross Stein, *We All Lost the Cold War* (Princeton, NJ: Princeton University Press, 1994), 51–55.

9. For example, see Richard Ned Lebow, *Between Peace and War: The Nature of International Crisis* (Baltimore: Johns Hopkins University Press, 1981); Michael Howard, *Studies in War and Peace* (New York: Viking Press, 1971), 99–109; Gerhard Ritter, *The Schlieffen Plan: Critique of a Myth* (London: Oswald Wolff, 1958); and D. C. B. Lieven, *Russia and the Origins of the First World War* (New York: St. Martin's Press, 1983).

10. Yaakov Katz, "Stuxnet virus set back Iran's nuclear program by 2 years," *Jerusalem Post*, 15 December 2010, http://www.jpost.com/LandedPages/PrintArticle.aspx?id=199475.

11. Ibid.

12. On the problem of attributing cyber attacks to their sources, see Libicki, *Cyberdeterrence and Cyberwar*, chap. 3, esp. 41–49 and passim.

13. Keith B. Payne, *Deterrence in the Second Nuclear Age* (Lexington: University Press of Kentucky, 1996), 57. See also David Jablonsky, *Strategic Rationality Is Not Enough: Hitler and the Concept of Crazy States* (Carlisle, PA: Strategic Studies Institute, 8 August 1991), esp. 5–8, 31–37.

14. Bruce G. Blair, *The Logic of Accidental Nuclear War* (Washington: Brookings Institution, 1993), 237.

15. Lebow and Stein, *We All Lost the Cold War*, 122–23.

16. Robert Jervis, *The Meaning of the Nuclear Revolution: Statecraft and the Prospect of Armageddon* (Ithaca, NY: Cornell University Press, 1989), 183.

17. Alexander L. George, "The Tension Between 'Military Logic' and Requirements of Diplomacy in Crisis Management," in *Avoiding War: Problems of Crisis Management*, 13–21, citation 18.

18. Ibid.

19. A virus is a self-replicating program intended to destroy or alter the contents of other files stored on floppy disks or hard drives. Worms corrupt the integrity of software and information systems from the "inside out" in ways that create weaknesses exploitable by an enemy.

20. Blair, *Logic of Accidental Nuclear War*, 252.

21. James G. March and Herbert A. Simon, *Organizations* (New York: John Wiley and Sons, 1958), 140, 146.

22. Lebow and Stein, *We All Lost the Cold War*, 335–36.

23. Graham T. Allison, *Essence of Decision: Explaining the Cuban Missile Crisis* (Boston: Little, Brown and Co., 1971), 141. See also Scott D. Sagan, *Moving Targets: Nuclear Strategy and National Security* (Princeton, NJ: Princeton University Press, 1989), 147; and Lebow and Stein, *We All Lost the Cold War*, 342.

24. For pertinent scenarios, see George H. Quester, *Nuclear First Strike: Consequences of a Broken Taboo* (Baltimore: Johns Hopkins University Press, 2006), 24–52. An escalation ladder with 44 rungs and seven major groups, from subcrisis maneuvering through civilian central wars with nuclear weapons, is defined in Herman Kahn, *On Escalation: Metaphors and Scenarios* (New York: Frederick S. Praeger, 1965), esp. 37–51.

25. Ibid., 27.

26. Assessments of deterrence before and after the Cold War appear in: Patrick M. Morgan, *Deterrence Now* (Cambridge: Cambridge University Press, 2003); Colin S. Gray, *The Second Nuclear Age* (Boulder, CO: Lynne Rienner, 1999); Keith B. Payne, *Deterrence in the Second*

Nuclear Age (Lexington: University Press of Kentucky, 1996); Robert Jervis, *The Meaning of the Nuclear Revolution: Statecraft and the Prospect of Armageddon* (Ithaca, NY: Cornell University Press, 1989); and Lawrence Freedman, *The Evolution of Nuclear Strategy* (New York: St. Martin's Press, 1981, 1983). Michael Krepon emphasizes that deterrence in the first nuclear age "worked," to the extent that it did so, only in conjunction with containment, diplomacy, military strength, and arms control. See Krepon, *Better Safe than Sorry: The Ironies of Living with the Bomb* (Stanford, CA: Stanford University Press, 2009), passim.

27. As David Alberts points out, "Information dominance would be of only academic interest, if we could not turn this information dominance into battlefield dominance." See Alberts, "The Future of Command and Control with DBK," in *Dominant Battlespace Knowledge*, eds. Stuart E. Johnson and Martin C. Libicki (Washington: National Defense University, 1996), 77–102, citation p. 80.

28. Lawrence Freedman, *The Evolution of Nuclear Strategy*, 3rd ed. (New York: Palgrave Macmillan, 2003), 463.

Cyberwar as a Confidence Game

Martin C. Libicki

Is CYBERWAR the twenty-first-century version of nuclear war? Readers of the *Economist*, whose 3–9 July 2010 cover portrayed a digitized nuclear explosion in the midst of a city, could be forgiven for thinking so. The takeaway was obvious: cyber weapons are now the latest class of strategic weapons, they can do enormous damage to societies, and the first recourse against this threat should be some sort of arms control. Otherwise, the bad old days of strategic confrontation would be back, but this time with scores of countries and no small number of nonstate actors, transnational criminal organizations, and a few overindulged high school students having the requisite capability to build weaponry that can bring life as we know it to a prompt halt.

Such a scenario could happen, but to see cyber weapons as primarily strategic in the same way as nuclear weapons is quite misleading. A more plausible strategic rationale for the United States' developing cyber weapons is to make *other* states think twice about going down the road toward network-centric warfare as the United States is doing, thereby extending its lead in this area. Cyber weapons do so by making other states—already lacking confidence in their ability to handle high technology—doubt that their systems will work correctly when called on, particularly if used against the United States or its friends.

This logic is explained in three parts, starting with a brief description of cyber attacks and their effects. Next, the case is made against assuming that cyberwar can be used for its strategic impact, followed by the case for thinking that the *threat* of cyberwar might possibly shape the investment decisions of other states to the advantage of the United States.

Martin C. Libicki, PhD, is a senior management scientist at RAND Corporation, focusing on the impacts of information technology on domestic and national security. He has published *Conquest in Cyberspace: National Security and Information Warfare and Information Technology Standards: Quest for the Common Byte*, as well as numerous monographs. Prior employment includes the National Defense University, the Navy Staff, and the GAO's Energy and Minerals Division. He holds a master's degree and PhD from the University of California–Berkeley.

Cyberwar: A Précis

There are critical differences between cyberwar and physical war.[1] These differences are so great that tenets about the use of physical force are imperfect guides to cyberspace. To summarize, cyberwar is the systematic use of information (bytes, messages, etc.) to attack information systems and typically, by so doing, the information that such a system holds.

Cyber attacks are enabled by (1) the exposure of target systems to the rest of the world, coupled with (2) flaws in such systems which are then exploited. Systems vary greatly in their susceptibility to cyber attacks, and such susceptibilities may also vary over time, especially before and after an attack. System owners are typically unaware of the exact nature of serious flaws of their own systems; otherwise they would not be flaws very long. They may not realize how exposed they are to the rest of the world. Yet, cyber attacks are self-depleting.[2] Once a vulnerability has been detected, often by dint of its being exploited and deemed consequential, efforts usually follow to eliminate the vulnerability or reduce a system's susceptibility to further such attacks.

The direct effects of cyber attacks are almost always temporary. Rarely is anything broken (the Stuxnet worm perhaps a prominent exception). At the risk of a little oversimplification, because a cyber attack consists of feeding systems the wrong instructions, replacing such instructions in favor of the original correct instructions returns control to the owner.[3]

The prerequisites of a cyber attack are clever hackers, cheap computer hardware, a network connection, intelligence on the workings and role of the target system, specific knowledge of the target's vulnerabilities, and the tools to exploit such vulnerabilities. Cheap computer hardware possibly aside, none of these can be destroyed in a cyber attack. Furthermore, none are the exclusive province of states, although states have distinct advantages in acquiring these prerequisites.

Cyber attacks are very difficult to attribute. Determining which machine or network the originating attack came from is challenging enough, but even knowing that much does not prove that its owner was responsible, because there are many ways for a hacker to originate an attack from someone else's box. Even finding the specific hacker does not necessarily prove that a state was responsible for his or her actions.

It is hard to predict the effects of cyber attacks, even those directed against well-scoped targets. Systems change constantly; processes that depend on affected systems' collateral damage are not readily apparent

and cannot necessarily be inferred from their physical properties. The ultimate cost of, say, a disruption is proportional to the time required to detect, characterize, and reverse its damage—all of which can vary greatly. Even after a cyber attack, it may not be clear what exactly happened; a data/process corruption attack, for instance, loses much of its force if the target knows exactly what was corrupted. What an attacker believes it did (much less its purpose) may differ from what happened, which in turn may differ from what the target perceived to happen.

Cyberwar does not sit on top of the escalation ladder, or even very close to the top. Thus, it is not necessarily the last word between states.

Cyber Warfare as Operational Warfare

Cyber attacks have a potentially important role to play against unprepared and unlucky adversaries that have enough sophistication to acquire and grow dependent upon information systems but not enough to defend them against a clever and persistent attack. Nevertheless, as suggested above, the effect of such an attack tends to be limited in time and scope. The fact that cyber attacks rarely break things means that the effects on systems are temporary. In that respect cyber warfare is, like electronic warfare, a facilitator of kinetic attacks. Indeed, both have been mooted against the same targets (e.g., SAMs). But electronic warfare has a serious advantage as a weapon that cyber weapons lack. It takes place outdoors, so to speak, where both sides contend for access to the same spectrum; factors such as the ability to generate a powerful signal can overwhelm a perfectly executed but weaker signal from the other side. To a first-order approximation, the environment is a given. Cyber warfare, however, takes place indoors, specifically in the systems of the target. Its ability to succeed has everything to do with the characteristics of the system being attacked. There is no forced entry, and a perfectly executed system is impenetrable; whereas perfection is not given to mortals, a completely disconnected, hence practically invulnerable, system is plausible.

Both electronic warfare and cyber warfare have relatively fast learning curves. Measure begets countermeasure begets counter-countermeasure and so on. But the cycles in cyberwar are faster and likely to lead to a permanently *lower* plateau of efficacy for the attacker. In cyberspace, the first attack is most likely to have significant effects, particularly if the attack itself is a strategic surprise (e.g., the preceding weeks were uneventful) so

that affected systems are operating in peacetime mode. Even if the attack were carried out against an alerted adversary, the possibility that the attacker knows of specific vulnerabilities that the defender overlooked means that some attacks may well get through. *After* the attack, however, the defender will realize that some of its systems were too exposed to the rest of the world or at least its other networks. It may well figure out the specific vulnerabilities that allowed such attacks to take place and fix or route around them. It will have a more nuanced understanding of how far to trust each of its information systems. As a result of all this, a second wave of attacks is likely to hit a higher wall, and less is likely to get through. The same logic of diminishing returns would characterize a third or fourth wave and so on. Thereafter, successful attacks tend to be those that would exploit newly found vulnerabilities—particularly in just-fielded systems.

Cyberwar as Strategic War

If cyberwar is going to assume strategic importance, it must be able to generate effects that are at least comparable to, and preferably more impressive than, those available from conventional warfare.[4] Can it?

There is a wide range of opinion on that score. People have worried about cyberwar for most of the last 20 years, and in all that time, not one person is known to have been killed by a cyber attack.[5] As for damage, estimates vary widely from several hundred million dollars a year to several hundred *billion* dollars a year. The most costly single attack was probably the "I Love You" virus in 2000, whose costs have been estimated at as much as $15 billion but which may be more realistically estimated at several hundred million dollars, if that.[6] Only one power plant is known to have been disabled by hackers—a system in southern Brazil in 2007—and even there, the power outage has been disputed by local authorities as soot buildup. The only two examples of a state's using cyber attacks against another were Russia's attacks against Estonia in 2007 and Georgia in 2008 (and Russia's responsibility is questionable in the first case); both caused disruption that can be measured at no more than the low millions of dollars, and both pulled their victims closer to rather than pushing them farther from NATO. The Stuxnet worm, if it worked, did serious damage, but it was closer in form to a onetime act of sabotage.

The depletion dynamic noted above would work in roughly the same way in the civilian world as it does in the military world. These days, networks

and systems are established with some degree of security adequate only to deal with the day-to-day threats such institutions face. Banks, for instance, give a great deal of thought to security in large part because the motive to rob them is ever present. Bank security is fairly good; bankers can reduce the damage to acceptable levels, which also puts a top bound on the damage a state-sponsored bank thief could carry out. Electric power companies, by contrast, are rarely attacked—what would be the point? Thus, unless they have been prodded to isolate themselves by the deluge of threat scenarios over the last few years, the difference between a state-level threat and today's threat could be quite substantial, and they may not necessarily be so well prepared. But, should state hackers appear, many such institutions would learn quickly that the threat environment had changed and, with more time, how to survive and cope with such change. Coping with the worst attacks might be expensive and disruptive. But, at the very worst, the most primitive response (sever all Internet connections) would return the US economy to the state that it had in the mid-1990s, before networking became so ubiquitous. Being cyber-bombed back to the 1990s has its downside, but it hardly compares to being bombed back to the Stone Age (pace LeMay) by conventional weaponry.

More to the point, for cyber to be a strategic weapon for coercive purposes, it has to be frightening to the population at large, or at least to their leaders—so frightening that the aggressors can actually reap some gains from the reaction or concession of their targets.[7] One motive for strategic cyberwar may be to threaten its use to modulate an ongoing conventional war—but that requires the effects of a cyber attack to be significant relative to the cost, casualties, and damage of violent conflict. Another may be straightforward coercion prior to a war. Imagine a scenario in which Taiwan declares its independence; the Chinese plan to take the island but want to forestall US intervention. China takes down power in a few US metropolitan areas as a way of suggesting that it can do worse (merely threatening to take down power may be much less impressive and hence less dissuasive, given the great uncertainties in what any given attack can do before one is demonstrated). So, would the United States accede to China's invasion of Taiwan? Or instead, would it regard the Chinese threat to be a strategic threat and thus regard the China-Taiwan struggle as strategic rather than local for having become entangled with that larger threat? US reactions to Pearl Harbor and 9/11 suggest the latter. Our strategists, in

turn, should not blithely assume other countries can be rolled even if we cannot be—those other countries can also be quite stubborn.

It follows that if the use of cyber weapons is unimpressive at the strategic level, the fear that might come from the *threat* to use cyber weapons may be similarly unimpressive. It is difficult to make credible threats because the efficacy of cyber weapons is strongly, perhaps overwhelmingly, determined by features of those systems such weapons are targeted against. Once such weapons are used successfully, their credibility goes up, but then the attacker (as well as the target) has to deal with the consequences of their *use* (e.g., open hostilities). Such consequences will complicate and may overwhelm the purely coercive/deterrent effect of threatening *subsequent* use.

Fear, Uncertainty, and Doubt

While the preceding discussion may create doubt about the strategic impact of cyberwar, there are other considerations with perhaps more long-term resonance. Consider the oft-conflated trinity of FUD: fear, uncertainty, and doubt.[8] Nuclear arms fostered fear, but there was not a great deal of doubt or uncertainty in their applications. Cyber may be the opposite—incapable of inducing real fear directly, but putatively capable of raising the specter of doubt and uncertainty. It can do so immediately by scrambling the data upon which decisions by man or machine are made. Its specter can do so latently. Inherent in the possession of consequential vulnerabilities is that their owners are unaware exactly which ones exist and what effect their exploitation may have—otherwise they likely would not be vulnerabilities for very long. It is virtually impossible to prove that any particular complex system exposed to the outside world (e.g., via the Internet) is not invulnerable or even uninfected. For all anyone knows, some code in such a system could be waiting for an explicit command or some internal circumstance (e.g., reaching a certain date/time or receiving a particular message) to force the system to fail. If there is an attack, the name of the attacker may not be known, much less its motive or purpose.

Keeping that point in mind, now backtrack to the dawn of the nuclear era. Until then, one could envision any state being disarmed and destroyed by another. Afterwards, it was impossible to conceive of a nuclear-armed state being destroyed (except by another willing to sacrifice most of itself

in the bargain), much less occupied. The most operationally offensive of weapons turned out to be the most strategically defensive weapon ever created. Ever since, the effective point of such weapons, to adulterate the famous phrase of Bernard Brodie, has been not to use them but to brandish them to make a point, to tell a story, as it were, about what were and were not a state's vital interests. In a mature strategic environment, the role of nuclear weapons was to become an element of narrative. The advent of terrorism and insurgency in the postwar era has strongly reinforced the role of narrative. Terrorism bills itself as the propaganda of the deed. Insurgency is currently local politics by other means. They are meant to lower the population's confidence in its own government. They, too, tell a story. Conversely, the primary thrust of US counterinsurgency doctrine is the use of armed forces to bolster such confidence—a different story.

Putting the two together sets the stage for delineating the purpose of *strategic* cyberwar. It, too, illustrates a narrative. There are many possible narratives available; many clearly have to do with confidence. A cyber attack that disables some infrastructure says as much about its reliability—the reliability of those who own, operate, or stand behind such infrastructures—as a physical attack. Those who would corrupt a state's banking system make a statement about the creditworthiness of the state and its citizens. The persistent presence of a cyberwar capability, if irritating enough, serves to taunt institutions. All this assumes, of course, an adversary talented enough and a set of system owners feckless enough to give credence to such a narrative.

The United States, for its part, generally has little interest in creating chaos or ruining the authority of other institutions, even if some regimes deserved as much. Societies that depend on cyber systems understand the risks of starting *that* fight.

Nevertheless, a US capability for offensive strategic cyber operations may actually be worthwhile. Start with the observation that a military that can collect, analyze, distribute, and make decisions on the basis of copious information is likely to do much better in combat than one that cannot. Such a vision has been increasingly demonstrated over the last 20 years, starting with the first Gulf War, wending its way through Bosnia, and culminating with Operations Allied Force, Enduring Freedom, and Iraqi Freedom. Even in today's difficult counterinsurgency environment, the advantages of networking remain. They allow time-urgent targeting and enable forces to learn faster from the experiences of one another.

Presumably, it would run counter to US interests for countries potentially hostile to the United States to pursue a similar strategy, one that becomes more attractive the more powerful information technology becomes. Might developing an offensive cyberwar capability be a way to induce hesitation in *their* efforts to lay a network foundation under their war fighting?

Here is where an uncertainty-and-doubt strategy comes into play. How would other states react to the idea that the United States—and it need not necessarily be us—could have hacked into their military systems and implanted code into their communications systems and perhaps even their weapons systems? Such code would lie dormant until precisely such time as the target state wishes to use its military—at which point the code is unleashed: communications cease to work reliably, messages sent across the network may or may not be authentic, the ability to keep state secrets or even operational details cannot be guaranteed. Weapons relied on to make war could fail. Even if no such code has been embedded beforehand, so much information could have been collected about target systems that hackers can reliably enter and confound such systems in time of crisis.

If systems of both sides have been corrupted, both might be embarrassed before third parties (to include potential adversaries looking for signs of weakness) by their mutual inability to carry out military operations. Perhaps the hacker picked sides—in which case, the correlation of forces on the battlefield will be far worse than the target state had anticipated. If the target state believes (1) that it has been so hacked, (2) it has no alternative but the systems and equipment it has, (3) its estimate of war's outcomes are decidedly worse as a result, and (4) it does have a choice on whether to go to war, then one might conclude that its desire to go to war would be reduced. Under these circumstances, the uncertainty-and-doubt strategy would have achieved the aims that only fear could accomplish in the nuclear context. War is inhibited.

How might such doubt and uncertainty be induced? The most straightforward way is to hack into such systems and then make it obvious that they have indeed been hacked. Exactly who would do such a thing is secondary, since the point is not to emphasize US prowess but the vulnerability of their systems—indeed any such systems—to cyber attack. If the point is to provide not proof but uncertainty, then making the result obvious beforehand is unnecessary. In fact, it may be unwise. Proving that the other side may be vulnerable requires revealing the vulnerability. But every exposure

leads to fixes, which makes the next exploitation much harder. Thus proving a system was, is, and remains forever hacked may be impossible. However, the hint of an attack leaves no specific trace and, hence, no specific fix. General fixes, such as selective disconnection or the installation of anti-malware guards, may be employed, but there will be nothing that suggests which of these general fixes will do the job. After all, it takes twice as long to find something as it does to find nothing—and that is only true if one believes that sweeping a space and finding nothing proves that nothing is there; if finding is conclusive but sweeping and finding nothing is inconclusive, then it takes far longer than twice as long to find something as opposed to not finding something. It may not be possible to be confident once some supposedly rogue code has been found, even after a great deal of effort has been put into the quest, particularly because it is never clear exactly what would distinguish unexplained code from the rogue code an adversary could plant. Such code could be a glitch unrelated to any malevolent actor. Arthur Clarke's tenet—any sufficiently advanced technology is indistinguishable from magic—applies here. It helps that many foreigners have convinced themselves that US intelligence agencies are omniscient. US cyber warriors need never single out the target of their magic, but just ensure there are enough hints out there that say they do, in fact, possess the requisite skills. For all anyone knows, foreigners actually believe as much of our cyber warriors, and any testable hint in that direction could fail and blow the fairy dust from their eyes. It cannot be overemphasized that the target of the attack is not the system but *confidence* in it or, indeed, any system.

The vulnerability of third-world states to such magic is enhanced to the extent that they have to purchase (or steal the plans for) their military systems. To be sure, there have always been advantages to rolling your own or at least being as sophisticated as those who supply you. Usually, though, the difference is a matter of degree rather than direction. The more sophisticated countries tend to be adept operators of their own equipment; unsophisticated nations, less so. Thus, an F-16 in the hands of an American pilot is likely to be more effective than in the hands of a typical third-world pilot. More analogously, an F-16 that is maintained by the United States is apt to be in better condition than a similar plane maintained by a third-world military. But even an inexpertly flown and indifferently maintained F-16 is a war machine.

When it comes to information systems, however, a cyberwar system of positive value in US hands could become a system of less positive value in the hands of a hostile third-world state, even a distinctly negative value. States that purchase sophisticated information technology need to know not only how to use and maintain it, but also how to defend it against cyber attack. The failure to defend may mean that such systems, under pressure, leak information, drop out unexpectedly, or provide misleading data to war fighters and other decision makers—with consequences that may be worse than if they had never bought and grown dependent upon such systems in the first place—particularly if the more-sophisticated networked system replaced a less-sophisticated stand-alone system. In information systems, quality has a quantity all its own. A great hacker is likely to be orders of magnitude more efficacious than a merely good one, in ways that do not characterize the difference between a great hardware repairman and a merely good hardware repairman. The inability of third-world countries to generate great cyber warriors may be attributed to poorer educational facilities and a less-educated recruitment base. Yet, their lack of access to others' source codes or their not having built any of their own (and having few among them who have ever built any operational source code) helps ensure their military systems are far more vulnerable to cyber attack than comparable systems of sophisticated states.

A state faced with such fears may try to manage by pursuing compensatory strategies. For instance, states may observe that the effects of cyber attacks are temporary and difficult to repeat. They then maintain their investment strategy after reasoning that even if their weapons do not work when first used, they can survive the initial exchange and gain requisite military value from their weapons on the second and subsequent rounds. If so, they would have to overlook the ability of high-technology militaries to conclude successful conventional campaigns over the course of days rather than months or years. That is, they may not get a second round. A sophisticated system owner may be able to find and patch a newly exploited vulnerability within hours or days after it has been discovered when the entire world is helping. But can an unsophisticated system owner, on the outs with the developed world, countering a sophisticated US cyber attack count on so quick a recovery? The state may also realize that once a system has become ill, war fighters may not want to bet their lives on it until it has been completely cured (a far lengthier process) rather than simply having its symptoms relieved.

If states anticipate that their networked systems may be penetrated, they may elect to foreswear the development of network-centric warfare. Why try to face foes with weapons that may well fail spectacularly if used? Why not rely on lower-tech weapons that are robust against cyber attack because of no network connections and perhaps not even much electronics? So, is an uncertainty-and-doubt strategy thereby defeated? Au contraire, it has triumphed without even requiring hackers to validate their skills. But, would success in dissuading a potential adversary away from a high-technology challenge to the United States actually be in its best interest? A great deal depends on the kinds of wars the United States wants to deter and/or conduct. If the goal is to make it very difficult for others to carry out a conventional invasion or mount a conventional defense, low-technology forces are no match against what the United States has—even if they have given US ground forces fits in Iraq and Afghanistan. Abjuring quality may provide others the means to pursue quantity, but so far, the trade-off for others has not been particularly good; quality done right usually triumphs.

Alternatively, states beset by uncertainty and doubt may load up on the electronics and double-check their bona fides against supply chain attacks but abjure networking. Or they may network their machines but not their war fighters, limiting a possible vector of cyber attack but preserving a high-tech edge. If so, the real question is whether they have given up something of real war-fighting advantage to retain sufficient confidence in the electronics they *do* buy. At that point in the argument, one must yield the podium to proponents of network-centric warfare to make their case. A great deal depends on how much war fighters gain by reaching out to one another to gather the knowledge required to wage war and learn from war's experience.

Does not Stuxnet prove that cyberwar is real rather than a narrative? A great deal depends on what the worm actually succeeded in doing. Although people understand how it worked, nearly everything else about it remains a mystery: who wrote it, for what end, and with what effect?[9] The most common (current) explanation is that the Israelis intended for it to get into and confound or destroy components in Iran's Natanz nuclear fuel centrifuge plant. Iran's reaction, however, merits note. Although Iranians initially denied that anything in the Bushehr nuclear power plant was affected by the worm, they arrested several individuals associated with the plant in the weeks after the worm attack and accused them of being spies. Given the stories that a Russian contractor may have been the initial injection

point for the worm, it may well have affected their ability to trust and thus work with such contractors. If Stuxnet did nothing more than make Iranians lose confidence in their nuclear projects, it may well have succeeded even if it "failed."[10]

With all this, the broader narrative stands. The information revolution has created new and radically more-effective ways of going to war. The United States has exploited these advantages. But network-centric warfare comes at a price, and that price is vulnerability to cyberwar. In essence, there is a new game, but it is one played at a very high level. Those who cannot play at that level may want to think twice about entering the game at that level—indeed about entering the game at all.

Such is the case for developing offensive cyberwar capabilities to inhibit the investment strategies of rogue states and others who would contest the United States militarily. Would such a strategy apply to Russia and China?

With Russia, the best answer is almost certainly not, for two reasons. First, Russian capabilities at cyber warfare are very advanced—as befits a state as interested as it has been in *maskirovka* and as blessed as it has been with a surfeit of world-class mathematicians. They may fear our capabilities but are unlikely to regard them as magic. Second, Russia's military long suit is *not* systems integration of complex electronics and networks. It is precisely because they lack confidence in their conventional military that they lean so heavily on their nuclear arsenal. Thus, it is unlikely that their investment strategy would be diverted by the United States' development of cyber weapons.

With China, the best answer is most likely no. The Chinese have certainly shown enthusiasm for cyberwar. It shows up in their doctrine and in the great volume of intrusions people attribute to them. In contrast to Russia, however, it appears that Chinese talents in cyberspace lean more toward quantity (as befits a focus on cyber espionage) than toward quality (as would be required to get into hardened military systems). Furthermore, China's military investment strategy is quite different from Russia's. It has less interest in achieving nuclear parity and more in pursuing antiaccess strategies that rely on sensors, surveillance, and missiles—which normally require high levels of systems integration, hence, networking. These factors leave some—but only some—scope for a US dissuasion policy based on cyberwar capabilities.

What of the reverse—can others use the threat of cyberwar to deprive the United States of the confidence it needs to pursue network-centric

warfare? True, the US military worries—a lot—about how the cyberwar capabilities of other states may undermine its own plans.[11] Indeed, the possibilities were raised 15 years ago,[12] although at that point the fears were more notional than real. But the United States realistically has no better path other than going forward. The actual dominance of network defense in the resourcing of the US Cyber Command says as much. The DoD is prepared to spend billions, perhaps tens of billions, of dollars in pursuit of information assurance, precisely because it has little alternative.

Inhibiting Economic Growth?

Although the prospect of cyber attack might also be used to inhibit similar investments in digitizing the civilian commercial economy, the nature of the threat is different. Militaries exist against the day that they are most needed. Economies work from one day to the next. So, the possibility that the threat of cyberwar might inhibit investment in networking is unlikely to apply to commercial systems. First, such systems are used often and are attacked often as well, usually by criminals and amateurs, giving their owners confidence they work most of the time. By contrast, one only knows whether military systems work when used in war, which is contingent and infrequent (training is different, because there is little advantage to the enemy in making such systems fail temporarily). Second, there is a global infrastructure of corporations that supply, service, and maintain commercial information systems of sufficient diversity and experience that one can have confidence in their work. Military systems, in contrast, are more likely to be indigenously maintained, particularly if the owner is shunned by the West or if turnkey product support is contingent on good behavior. Third, the rationale for deepening the digitization of commercial and civilian systems is fairly straightforward and can be constantly validated in the day-to-day marketplace; cyber attacks constitute one risk that has to be factored into using them. The rationale for military digitization, especially by countries less involved in combat is far more speculative; there is a great deal of faith and emulation going into such decisions. By contrast, the effects from relying on digitization and then losing everything in a cyber attack when most needed—even if only for a few days—could be catastrophic.

Concluding Thoughts

In the 1970s, Thomas Wolfe "discovered" that modern art had "become completely literary: the paintings and other works exist only to illustrate the text."[13] Aesthetics aside, one can argue that cyberwar may have assumed a similar status, at least those acts of cyberwar that do not directly support military operations. It has become the latest manifestation of a trend that, when it comes to the means of war, what you do with it has become less important than what you say with it. Thus, the nuclear era was all about deterrence not combat, while more-modern cyber-limited conflicts are meant to serve as warnings. Building up our offensive capabilities is a confidence game. It says to those who would compete in our league: are you confident enough in your cyberwar skills that you can build your military to rely on information systems and the machines that take their orders? SSQ

Notes

1. For greater explanation, see Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009), chap. 2.

2. Depletion (of cyber tricks) could mean one or more of several phenomena: (1) there are only so many tricks and they have been exhausted or (2) the best tricks have been played but what remain (a) produce results that are less useful or easier to recover from before much has been damaged, (b) work with less likelihood, or (c) work under fewer circumstances whose occurrence is less likely (e.g., the target machine is not in the required state very often). Alternatively, the time required to find the next good trick grows steadily longer.

3. One major exception is a cyber attack on a system that has yet to work correctly and thus has no proven set of correct instructions and hence no baseline to return to.

4. Inasmuch as nuclear weapons could end life on Earth and cyber weapons cannot, relegating cyberwar to, at best, a second-level strategic weapon seems to be an easy assertion.

5. Eleven people were said to have died as a result of the Northeast power outage in 2003. The outage was reportedly hastened because the Slammer worm disabled warning systems at First Energy, but subsequent investigation has largely discredited the connection.

6. The best guess may be more than 10 million individuals lost about an hour's worth of productivity. Evan Hansen, "Poll finds few affected by 'I Love You' Virus," *cnet.com*, http://news.cnet.com/Poll-finds-few-affected-by-I-Love-You-virus/2100-1023_3-241539.html.

7. The attacks of 9/11 seem to have liberated many strategists from having to ask what advantage attackers would reap from their actions—saying "they do not like us" seems to suffice. That noted, there has yet to be any act of cyber terrorism that has gone beyond defacing websites.

8. This term was coined by Gene Amdahl, after he left IBM to found his own eponymous company, to refer to the "fear, uncertainty, and doubt that IBM sales people instill in the minds of potential customers who might be considering Amdahl products."

9. Note how it took at least three corporations—VirusBlokAda (a security firm based in Belarus), Symantec (a US security firm), and Siemens (a manufacturer of industrial electronics)—

to contribute important pieces to determining how Stuxnet worked and how to ensure that copycats would not.

10. Iran's leader reported that centrifuges at Natanz were damaged. Thomas Erdbrink, "Ahmadinejad: Iran's nuclear program hit by sabotage," *Washington Post*, 29 November 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/11/29/AR2010112903468.html. This, after months of denial, lent credence to the claim that Stuxnet did what it was designed to do but is no proof if one believes that Iran's leadership saw political advantage in blaming others for their own mistakes.

11. William J. Lynn, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* 89, no. 5 (September/October 2010): 97–108.

12. David Alberts, *Defensive Information Warfare* (Washington: National Defense University Press, 1996).

13. Thomas Wolfe, *The Painted Word* (New York: Bantam, 1977). The *Harper's* magazine article that excerpted the quotation begins nicely with his trip to an art exhibit in which, as one might expect, the pictures are large and the description-cum-explanation next to them are the size of a note card. He concludes by saying that if modern art were properly understood, the explanations would be wall-sized and the painting itself the size of note cards, merely an illustration of the narrative.

2011 CSAF Reading List

First Quarter Recommendations from General Schwartz

Three Cups of Tea: One Man's Mission to Promote Peace … One School at a Time, by Greg Mortenson and David Oliver Relin, is part of the leadership category and offers an account of a dedicated individual striving to establish peace in Central Asia one school at a time.

Technology Horizons: A Vision for the Air Force Science and Technology, by Dr. Werner Dahm, is a selection from the strategic context category that highlights the need for Airmen to anticipate emerging science and technology advances that have the greatest military potential.

The All Americans, by Lars Anderson, is featured in the military heritage category and gives a unique insight into the lives of four football stars who, after playing each other in the 1941 Army-Navy football game just days before the attack on Pearl Harbor, were later united in fighting the Axis powers during World War II.

Other Books in This Year's Reading List

Leadership

***Partners in Command: George Marshall and Dwight Eisenhower in War and Peace*, by Mark Perry**
***The Lost Peace: Leadership in a Time of Horror and Hope, 1945-1953*, by Robert Dallek**
***Secrets of Special Ops Leadership: Dare the Impossible; Achieve the Extraordinary*, by William Allen Cohen**

Strategic Context

***Monsoon: The Indian Ocean and the Future of American Power*, by Robert D. Kaplan**
***Cyber War: The Next Threat to National Security and What to Do About It*, by Richard A. Clarke and Robert Knake**
***The Return of History and the End of Dreams*, by Robert Kagan**
***A Savage War of Peace: Algeria 1954-1962*, by Alistair Horne**
***Descent into Chaos: The United States and the Failure of Nation Building in Pakistan, Afghanistan and Central Asia*, by Ahmed Rashid**

Military Heritage

***Fighter Pilot: The Memoirs of Legendary Ace Robin Olds*, by Robin Olds, Christina Olds, and Ed Rasimus**
***Red Eagles: America's Secret MiGs*, by Steve Davies**
***Cataclysm: General Hap Arnold and the Defeat of Japan*, by Herman S. Wolk**

for more information

http://www.af.mil/information/csafreading/index.asp

Book Reviews

Cyberdeterrence and Cyberwar by Martin C. Libicki. RAND, 2009, 244 pp., $33.00.

A cynic might sum up the US approach to information-age national security by paraphrasing Mark Twain's observation about weather—everybody talks about cyberspace, but nobody does anything about it. To refute such an observation, *Cyberdeterrence and Cyberwar* aims to inform the establishment of US Cyber Command and its service components. This monograph, based on Air Force–contracted research by the RAND Corporation, examines whether deterrence and war-fighting tenets established in traditional combat media (air, sea, and land) translate into the medium of cyberspace. Dr. Martin Libicki, is a senior management scientist at RAND who focuses on security impacts of information technology. His portfolio includes many cyberspace-related works; *Defending Cyberspace and Other Metaphors* (1997), written during his 12 years at the National Defense University, contains essays that foreshadow the findings of this book.

Libicki's thesis is straightforward: "to focus on the policy dimension of cyberwar" and explore "key aspects of cyberwar to establish a framework for considering cyberdeterrence." His primary audience is USAF leadership tasked to create its new cyberspace structure. Many of Libicki's findings are controversial. He argues that "there is no forced entry in cyberspace" because "organizations are vulnerable to cyberattack only to the extent they want to be." He also asserts that "cyberwar operations neither directly harm individuals nor destroy equipment" and thus can only play a niche role. Further, he contends, "strategic cyberwar is unlikely to be decisive" to induce political compliance, as compared to strategic airpower. Regarding deterrence, he concludes, "cyberdeterrence may not work as well as nuclear deterrence" due largely to its ambiguities compared to the "clarity of nuclear deterrence."

While there are weaknesses in Libicki's supporting arguments, there is considerable merit to the structure of his analysis. The initial chapters establish a systematic framework for subsequent examination. Cyberspace is a virtual medium of three layers—physical (hardware), syntactic (machine operating software), and semantic (the actual information). Cyber attack is the "deliberate disruption or corruption by one state of a system of interest to another state"; it does not include computer network exploitation (spying). This monograph limits cyberdeterrence to the principles of deterrence by punishment, defining it as "a capability in cyberspace to do unto others what others may want to do unto us." Libicki devotes a chapter to "Why Cyberdeterrence is Different," in which he assesses nine simple yet profound questions that flesh out his views and biases. These questions deserve extensive dialogue within the national security community.

Other chapters on cyber attack motivations and responses offer thoughtful reflections considered from the defender's and attacker's perspectives.

Turning to strategic cyberwar, Libicki restricts his arguments to state-on-state cyber attacks and excludes physical warfare as well as legal, diplomatic, and economic elements. He claims that cyberwar cannot "disarm, much less destroy, the enemy" and minimizes its consequences with debatable statements such as "most government computers can go down for several weeks with only minor inconvenience to the average citizen" and "systems can be set straight painlessly." Posing that strategic cyberwar activities are more likely to agitate than frighten an opponent, Libicki concludes it is "hard to argue that the ability to wage strategic cyberwar should be a priority area for U.S. investment."

The author presents operational cyberwar as a possible "decisive force multiplier" but elects not to include physical attacks on networks, electronic warfare, and psychological operations in his discussion. Not surprisingly, Libicki declares that operational cyberwar "cannot win an overall war on its own," therefore "the question of cybersupremacy is meaningless." Similarly, his discussion of cyber defense specifically distinguishes between military and nonmilitary system defense measures, proposing that only militaries have enemies, thus the need to be prepared for extraordinary circumstances. Ironically, many principles of defense he presents could easily be applied to nonmilitary systems as well.

Understanding the context of state (or nonstate) conflict apropos to developing cyberspace policy requires an integrated approach. A significant element of deterrence and war missed by Libicki regards how state sovereignty is defined in cyberspace. Another shortfall is his choice to compartmentalize military aspects of cyberspace from other instruments of national power (diplomatic, economic, information). Libicki's book also builds on a critical oversimplification: the prevalent assumption that nuclear deterrence and physical warfare are linear and well defined, but in contrast, deterrence and war in cyberspace are uniquely ambiguous (and therefore not subject to historical analysis). To exacerbate the contentious nature of his premise, the author downplays the primary impacts of cyberspace activities without fully characterizing possible second- and third-order effects—to wit, his claim that "the effects of cyberattack are temporary" is hard to accept at face value.

Granted, Libicki has courage to advocate views at odds with popular "gloom and doom" cyberspace scenarios painted by many authors. In reality the truth lies somewhere in between, and perhaps advocates of both extremes first should evaluate where cyberspace notions are similar before espousing perceived differences. Sadly, Libicki falls into a common trap among present authors—his text often confuses and dilutes his arguments with new words created simply by adding "cyber" as a prefix and providing no definition. For clarity, future discourse should refrain from the cyber–name game and only use the term *cyberspace*, if possible (for example, by changing this book title to *Deterrence and War in Cyberspace*). This serves more than semantic niceties; having intentional nomenclature can help achieve unity of effort within a fledgling unified Cyber Command.

Despite its foibles, *Cyberdeterrence and Cyberwar* is not a feckless work. It identifies many issues and concepts relevant to strategic and operational cyberspace operations which require thoughtful and collaborative discourse. However, readers should realize that many of its arguments downplay the significance of cyberspace in a military environment and do not address complex interactions among all elements of national power. As such, it does not provide sufficient analysis upon which decision makers should act, but it can provide value as one voice within a broader dialogue.

COL Jeffrey L. Caton, USA, Retired
Army War College

Cyberpower and National Security edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz. Potomac Books, 2009, 642 pp., $39.95.

Not long ago, cyberspace was viewed as a realm for each service's tech wizards, relegated to support land, sea, air, and space domains. This was partly due to service and joint doctrines not articulating until recently that conflicts can be waged in the cyber domain or that cyber power is a necessary part of the national power arsenal. The increasing volume and severity of attacks on the national and military cyber infrastructure dramatically changed that view. Cyberspace has now taken a prominent role in the military as a fifth, coequal domain of warfare.

With this recognition has come a shift in organizational structures and priorities. The secretary of defense formed a sub-unified combatant command, US Cyber Command, under US Strategic Command; the Air Force stood up a Numbered Air Force dedicated to cyberspace; and the Navy stood up its own cyber command.

These changes in the military did not happen in a vacuum. As the world, and particularly the United States, has become more dependent on the Internet for commerce, military operations, and so forth, senior decision makers realized that the future of the military and the nation hinges on securing cyberspace and developing cyber power. A prominent think tank, the Center for Strategic and International Studies, released a report in winter 2008 outlining what it believed were the pertinent issues the new president needed to address with regard to cyberspace. The new administration also commissioned its own study to develop a roadmap for national cyberspace priorities.

Despite these prominent organizational moves, the theories, definitions, and deep understanding of this new domain remain a mystery to many military leaders and strategists. The strategic dialog has been hampered by a lack of generalists who completely understand this domain and because much of the discussion about cyberspace and cyber power is shrouded in secrecy by the government and military. Some in academia and the military believe that serious strategic thinking about cyber power is at its infancy, much like airpower theory was during the interwar period.

Cyberpower and National Security attempts to fill the need for more strategic dialog on cyberspace and cyber power so more leaders, strategists, and practitioners

can learn and contribute to the discussions. It grew out of the Department of Defense's 2006 *Quadrennial Defense Review* when the DoD realized that it lacked the necessary intellectual tools to assess cyber power issues. The DoD tasked the National Defense University to help articulate cyber power in terms of national security. The result was a compendium of 24 articles authored by academics, think tanks, government cyber experts, and industry players who looked at areas as diverse as fundamental definitions to cyber deterrence theory to international law. The editors of *Cyberpower and National Security* arranged the articles to help frame the diverse discussion topics as well as to help readers gain a better understanding of cyberspace, even if their knowledge level of the domain was minimal.

Despite the range of topics, a common message does emerge. That message is that the cyber domain is complex, evolving, and demands additional serious study. No single volume, *Cyberpower and National Security* included, can hope to completely fill this gap. The articles are intended to give readers a glimpse of the myriad issues which play significant roles in national security and military strategy but are rarely discussed in sufficient detail for strategists and senior leaders to understand how to deal with them effectively.

Cyberpower and National Security is a groundbreaking book because of its depth and breadth and should become a standard volume which many military leaders and strategists will want to read and refer to for years to come. War colleges and civilian universities will also find it helpful to incorporate into their strategy and cyberspace curricula. If this volume serves its intended purpose, some readers will be inspired to investigate the topics further and use it as a launching point for additional studies or discussions.

Col Rizwan Ali, USAF
US Strategic Command

The Essential Herman Kahn: In Defense of Thinking edited by Paul Dragos Aligica and Kenneth R. Weinstein. Lexington Books, 2009, 286 pp., $29.95.

The Essential Herman Kahn is an anthology of previously published material from the professional life of Herman Kahn and illustrates a wide spectrum of thought-provoking issues that may affect our roles and responsibilities in society. Throughout, Kahn offers well-crafted arguments on important issues and presents new insights into the realms of political science, public policy, military strategy, and decision making.

Kahn was first recognized as a nuclear strategy theorist and later expanded his interest into the broader issues of public policy as a futurist. During World War II, he was stationed in Burma as a communications specialist for the US Army Signal Corps. After the war he completed his undergraduate degree in physics at UCLA. During the early 1950s at the RAND Corporation in California, he contemplated the emerging impact of nuclear weapons being placed into the American military arsenal. Kahn articulated the use of these weapons in a manner

that surprised some people and offended others. He is considered by some as the model for Stanley Kubrick's title character in the movie "Dr. Strangelove." After RAND, he began his own "think tank" called the Hudson Institute in 1961.

Kahn pondered the uses and effects of the employment of nuclear weapons during a military confrontation between the United States and the Soviet Union. He espoused the theory that the "world" could survive a total nuclear war—a concept alien to the generally accepted theory that a nuclear weapon exchange between the world's two superpowers would end civilization as we knew it. Kahn offered a different lens from which to view the horrific cataclysmic effects of a total nuclear war—that the result of a nuclear exchange of weapons, while it would greatly change the world as we knew it, would not destroy it. His theory was not widely accepted, and Kahn was labeled a free thinker, not bound by the usual protocols. Critics charged that his theories were reckless for merely discussing the likelihood of a nuclear exchange and may well have made such an exchange more likely. Kahn dismissed this argument as foolhardy and counterproductive. He postulated that educating the populace of the true effects of nuclear warfare was more important to prevention than a self-fulfilling prophecy. Kahn also stated the world needs to discuss matters of importance and not avoid topics simply because they may frighten readers.

The Essential Herman Kahn offers a banquet of thought on nuclear weapon strategy. This book reflects the breadth of topics on which Kahn wrote and spoke during his tenure at RAND and the Hudson Institute, including economic growth, cultural change, policy research, decision making, and forecasting the future. This list offers insight into the perspective Kahn brought to analysis—he seems to measure the topics as interconnected and relates the impact or intentions in one arena to the effects in another.

This is not a light work for a casual read but a thoughtful piece that shall absolutely capture the reader's attention. While one must invest full attention to the thoughts expressed by Kahn to fully comprehend his reasoning, the payback is worth the effort. The vocabulary is similar to a college textbook or a magazine commentary; whereby, Kahn explores each topic in sufficient detail that the reader is enriched with a new perspective. The value of the book lies in its presentation of topics that educate, inform, and perhaps motivate the reader to ponder the merits of the arguments offered. Again, this is not an easy read; however, the journey through its pages will add to personal knowledge on the topics and force readers to reassess their own beliefs. That is the value of reading the book.

Col Joe McCue, USAF, Retired
Leesburg, Virginia

Mission Statement

Strategic Studies Quarterly (SSQ) is the senior United States Air Force–sponsored journal fostering intellectual enrichment for national and international security professionals. *SSQ* provides a forum for critically examining, informing, and debating national and international security matters. Contributions to *SSQ* will explore strategic issues of current and continuing interest to the US Air Force, the larger defense community, and our international partners.

Disclaimer

The views and opinions expressed or implied in the *SSQ* are those of the authors and should not be construed as carrying the official sanction of the United States Air Force, the Department of Defense, Air Education and Training Command, Air University, or other agencies or departments of the US government.

Comments

We encourage you to e-mail your comments to us at: **strategicstudiesquarterly@maxwell.af.mil**. We reserve the right to edit your remarks.

Article Submission

The *SSQ* considers scholarly articles between 5,000 and 15,000 words from United States and international authors. Please send your submission in Microsoft Word format via e-mail or regular mail (hard copy and a CD) to:

e-mail: **strategicstudiesquarterly@maxwell.af.mil**

Strategic Studies Quarterly (SSQ)
Managing Editor
155 N. Twining Street, Building 693
Maxwell AFB, AL 36112-6026
Tel (334) 953-1108
Fax (334) 953-1451

Visit *Strategic Studies Quarterly* online at **http://www.au.af.mil/au/ssq/**

Free electronic subscription at **http://www.af.mil/subscribe**

SSQ SPECIAL EDITION

Cyber

"Aim High . . . Fly-Fight-Win"